CITY OF OAKLAND

Privacy Advisory Commission

April 7, 2022 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Jessica Leavitt*

Pursuant to California Government Code section 54953(e), Oakland Privacy Advisory Commission Board Members/Commissioners, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

TO OBSERVE:
Please click the link below to join the webinar:
https://us02web.zoom.us/j/85817209915
Or iPhone one-tap:
US: +16699009128, 85817209915# or +13462487799, 85817209915#
Or Telephone:
Dial (for higher quality, dial a number based on your current location):
US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 646 558 8656
Webinar ID: 858 1720 9915
International numbers available: https://us02web.zoom.us/u/kDUn0z2rP

TO COMMENT:
1) To comment by Zoom video conference, you will be prompted to use the "Raise Your Hand" button to request to speak when Public Comment is being taken on the eligible Agenda item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

2) To comment by phone, you will be prompted to "Raise Your Hand" by pressing "* 9" to request to speak when Public Comment is being taken on the eligible Agenda Item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.
ADDITIONAL INSTRUCTIONS:
1) Instructions on how to join a meeting by video conference is available at: https://support.zoom.us/hc/en-us/articles/201362193%20-%20Joining-a-Meeting#
2) Instructions on how to join a meeting by phone are available at: https://support.zoom.us/hc/en-us/articles/201362663%20Joining-a-meeting-by-phone
3) Instructions on how to "Raise Your Hand" is available at: https://support.zoom.us/hc/en-us/articles/205566129-Raising-your-hand-In-a-webinar

1. Call to Order, determination of quorum

2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings

3. Review and approval of the draft March meeting minutes

4. Open Forum/Public Comment

5. Privacy Commission Ordinance – annual election of chair/vice-chair positions

6. Federal Task Force Ordinance – OPD – Presentation of Annual Reports (ATF, USMS, DEA)
    a. Review and take possible action on reports

7. Sanctuary Contracting Ordinance – CPO – Presentation of Annual Report
    a. Review and take possible action on report

8. AB 2336 (Friedman) Speed Safety System Pilot Program – Safer Streets LA/National Motorists Association – Informational report only
    a. No formal action will be taken on this item at this meeting

9. Surveillance Equipment Ordinance – OPD – Crime Analysis Software
    a. Review and take possible action on Impact Report and proposed Use Policy

10. Surveillance Equipment Ordinance – OPD – Biometric Crime Lab – Informational report only
    a. Review proposed San Francisco ordinance (Sup. Ronen)
    b. Review existing policies and proposed state laws (SB 1228)
    c. No formal action will be taken on this item at this meeting

11. Surveillance Equipment Ordinance – EDW – East Oakland Security Camera Proposal
    a. Review and take possible action on Impact Report and proposed Use Policy

12. Surveillance Equipment Ordinance – OPD – Annual Reports (Automated License Plate Readers, Cell-Site Simulator, Biometric Crime Lab, Forensic Logic/Coplink, GPS Tag Tracker, ShotSpotter, Live Stream Camera, Mobile Fingerprint ID, Unmanned Aerial Vehicles/Drones)
    a. Review and take possible action on the reports

OAKLAND PRIVACY ADVISORY COMMISSION

RESOLUTION NO. __2_____

ADOPT A RESOLUTION DETERMINING THAT CONDUCTING IN-PERSON MEETINGS OF THE PRIVACY ADVISORY COMMISSION AND ITS COMMITTEES WOULD PRESENT IMMINENT RISKS TO ATTENDEES' HEALTH, AND ELECTING TO CONTINUE CONDUCTING MEETINGS USING TELECONFERENCING IN ACCORDANCE WITH CALIFORNIA GOVERNMENT CODE SECTION 54953(e), A PROVISION OF AB-361.

WHEREAS, on March 4, 2020, Governor Gavin Newsom declared a state of emergency related to COVID-19, pursuant to Government Code Section 8625, and such declaration has not been lifted or rescinded. *See* https://www.gov.ca.gov/wp-content/uploads/2020/03/3.4.20-Coronavirus-SOE-Proclamation.pdf; and

WHEREAS, on March 9, 2020, the City Administrator in their capacity as the Director of the Emergency Operations Center (EOC), issued a proclamation of local emergency due to the spread of COVID-19 in Oakland, and on March 12, 2020, the City Council passed Resolution No. 88075 C.M.S. ratifying the proclamation of local emergency pursuant to Oakland Municipal Code (O.M.C.) section 8.50.050(C); and

WHEREAS, City Council Resolution No. 88075 remains in full force and effect to date; and

WHEREAS, the Centers for Disease Control (CDC) recommends physical distancing of at least six (6) feet whenever possible, avoiding crowds, and avoiding spaces that do not offer fresh air from the outdoors, particularly for people who are not fully vaccinated or who are at higher risk of getting very sick from COVID-19. *See* https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html; and

WHEREAS, the CDC recommends that people who live with unvaccinated people avoid activities that make physical distancing hard. *See* https://www.cdc.gov/coronavirus/2019-ncov/your-health/about-covid-19/caring-for-children/families.html; and

WHEREAS, the CDC recommends that older adults limit in-person interactions as much as possible, particularly when indoors. *See* https://www.cdc.gov/aging/covid19/covid19-older-adults.html; and

WHEREAS, the CDC, the California Department of Public Health, and the Alameda County Public Health Department all recommend that people experiencing COVID-19

symptoms stay home. *See* https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/steps-when-sick.html; and

WHEREAS, persons without symptoms may be able to spread the COVID-19 virus. *See* https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html; and

WHEREAS, fully vaccinated persons who become infected with the COVID-19 Delta variant can spread the virus to others. *See* https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html; and

WHEREAS, the City's public-meeting facilities are indoor facilities that do not ensure circulation of fresh / outdoor air, particularly during periods of cold and/or rainy weather, and were not designed to ensure that attendees can remain six (6) feet apart; and

WHEREAS, holding in-person meetings would encourage community members to come to City facilities to participate in local government, and some of them would be at high risk of getting very sick from COVID-19 and/or would live with someone who is at high risk; and

WHEREAS, in-person meetings would tempt community members who are experiencing COVID-19 symptoms to leave their homes in order to come to City facilities and participate in local government; and

WHEREAS, attendees would use ride-share services and/or public transit to travel to in-person meetings, thereby putting them in close and prolonged contact with additional people outside of their households; and

WHEREAS, on October 7, 2021, the Privacy Advisory Commission adopted a resolution determining that conducting in-person meetings would present imminent risks to attendees' health, and electing to continue conducting meetings using teleconferencing in accordance with California Government Code Section 54953(e), a provision of AB-361; now therefore be it:

RESOLVED: that the Privacy Advisory Commission finds and determines that the foregoing recitals are true and correct and hereby adopts and incorporates them into this resolution; and be it

FURTHER RESOLVED: that, based on these determinations and consistent with federal, state and local health guidance, the Privacy Advisory Commission renews its determination that conducting in-person meetings would pose imminent risks to the health of attendees; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission firmly believes that the community's health and safety and the community's right to participate in local government, are both critically important, and is committed to balancing the two by continuing to use teleconferencing to conduct public meetings, in accordance with California Government Code Section 54953(e), a provision of AB-361; and be it

FURTHER RESOLVED: that the Privacy Advisory Commission will renew these (or similar) findings at least every thirty (30) days in accordance with California Government Code section 54953(e) until the state of emergency related to COVID-19 has been lifted, or the Privacy Advisory Commission finds that in-person meetings no longer pose imminent risks to the health of attendees, whichever occurs first.

CITY OF OAKLAND

Privacy Advisory Commission

March 3, 2022 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair **Mayoral Representative**: Jessica Leavitt*

---

1. Call to Order, determination of quorum

Members Present: Katz, Oliver, Suleiman, Hofer, Tomlinson

Chair Hofer also introduced new Member Leavitt who was confirmed by the City Council but not yet sworn in. she will begin serving officially next month.

2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings

The resolution was adopted unanimously.

3. Review and approval of the draft December meeting minutes

The minutes were approved unanimously.

4. Open Forum/Public Comment

There were three public speakers:

J.P. Masser expressed concern about recently cancelled meetings, suggesting the public should have a better explanation for their cancellation. He also is concerned about the lack of Equipment Reports coming forward in the past 6 months.

*Nino Parker raised a concern about cameras that have been installed on light poles on Lakeshore Avenue in the cul-de-sac area and their impact on people's privacy. *staff noted that these cameras were NOT installed by the City and the City does not know who installed them.*

Assata Olugbala raised concerns about privacy at a recently established City homeless intervention, the Lake Merritt Tiny Homes, she also is concerned about gentrification pushing black people away from Lake Merritt.

5. Federal Task Force Ordinance – OPD – Review Annual Reports (ATF, USMS, DEA, FBI Child Exploitation and Violent Crime, Secret Service)

Chair Hofer opened this item with questions about any expired MOUs, noting that they would need to come back to the PAC and Council. Captain Holmgren noted he was aware of only the DEA MOU being expired, but staff would check each of them before returning to the PAC.

Member Suleiman asked about the ongoing training of officers involved in these task forces and Captain Holmgren noted they participate in 40 hours of POST training each year along with additional departmental trainings.

Member Katz noted an error in the FBI report for correction, Chair Hofer asked for clarity regarding the use of surveillance equipment: the DEA and Secret Service reports state none was used but further in the reports there are references to wire taps. He asked that this be clarified.

Chair Hofer also inquired about the arrest of females in trafficking cases cited in the Child Exploitation task Force Report. Sgt. Campos explained that the department does nor criminalize juveniles that are being trafficked but does use an arrest as a way to get the victims into immediate services including safe housing where their trafficker cannot locate them.

Last, Chair Hofer raised a long-standing concern about the many reports referencing CA Penal Code 832.7: the department consistently references this statute as reason to not report whether any violations of policy were committed by the officers involved in the task force. The argument made in the past is that if one officer is assigned and a violation is reported, it will expose that officer in violation of CA Penal Code 832.7 which prohibits the release of such information in a public hearing. Chair Hofer asked OPD to cite the legal authority that OPD is using and if they cannot, that they modify this section of all of the reports.

There was one Public Speaker on the item: Assata Olugbala asked about a home for girls that was located in Council District 7 that abruptly closed down.

The reports were tabled to next month for approval after the issues raised are addressed.

6. Surveillance Equipment Ordinance – OPD – Crime Analysis Software

Nicole Freeman, Manager of OPD's Crime Analysis Unit presented on the item.

Chair Hofer addressed several sections of the Impact Statement that require attention: Under Section A he noted the PAC would need to see the training manual as it is in those manuals that discoveries of prohibited uses are sometimes discovered. In Section C he would like to see some crime stats, in Section H he asked if there were any proposed or operative contracts that could be shared with the PAC (as required by the ordinance), and in Section I he wanted to see more information about third party access which is always a concern.

Nicole explained the handbook is embedded in the software and it was agreed the ad hoc committee that will go into detail will meet online so they can view the handbook on her screen.

In the Use Policy, Chair Hofer had several questions about the databases and access. Nicole explained that there is no connection to outside databases, and no data sharing as this is an internal product. She went on to explain how the tool is used, citing an example of tracking auto burglaries in Jack London Square. She explained the focus is on the geographic data and trends and can actually help reduce disparate enforcement. Member Tomlinson had questions about how the data is pulled in and aggregated, noting that if there is already disparate enforcement that the data is based on, it could create bias. She also asked about data manipulation. Nicole explained that the data is queried geographically to help the department determine where to deploy.

There were two public speakers on the item: Assata Olugbala expressed her concern that racism can seep in anywhere so even though this technology is about geography, the PAC should still be wary. Nino Parker echoed those sentiments, noting that the OPD Stop Data still shows huge disparities in how often Black people are stopped versus others.

An ad hoc committee was formed to work with staff that includes Members Tomlinson, Katz, Oliver, and Hofer. The item was continued to next month.

The meeting adjourned at 6:33pm.

OAKLAND POLICE DEPARTMENT
Alcohol Tobacco and Firearms (ATF)
2021 Annual Report

OPD ATF Taskforce

The OPD ATF Taskforce supports firearm related investigations. The firearm investigations are often associated with Crime Guns identified through the National Integrated Ballistic Information Network (NIBIN), unserialized firearms (Ghost Guns), Convicted Felons in possession of firearms and the tracing or tracking of firearms through E-Trace. The Taskforce also provides OPD CID with access to forensic resources to support investigations involving gun violence in Oakland. The Taskforce also provides resources to the OPD Crime Gun Intelligence Center (CGIC). OPD CGIC utilizes the National Integrated Ballistic Information Network (NIBIN), which provides crucial intelligence about firearms related crimes committed in Oakland and the San Francisco Bay Area. ATF Special Agents and OPD Taskforce Officer/s frequently respond to assist several Bay Area Law Enforcement Agencies and the Oakland Police Department to conduct investigations of individuals or groups who victimize Oakland residents. The Taskforce also supports the Ceasefire program in the adoption of State firearm cases involving repeated violent Felons identified through Ceasefire.

Staffing

1. **Number of full and part time OPD officers assigned to ATF Task Force:** One part-time Officer. One full-time NIBIN analyst is currently assigned to OPD to assist with analytical data related to NIBIN Investigations.
2. **Number of hours worked as ATF Task Force Officer**: Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there are active investigations.
3. **Funding source for ATF Task Force Officer salary**: OPD Budget – funded by OPD General Purpose Fund. Overtime related to ATF OPD Taskforce investigations are funded by the ATF.

Other Resources Provided

1. **Communication equipment:** ATF handheld radio, cellular phone & laptop computer.
2. **Surveillance equipment:** ATF owns and installs utility pole cameras which are utilized in some cases. A court order w/ judicial approval is required prior to any installation.
3. **Clerical/administrative staff hours:** NIBIN Analyst: Regular 40 hours per week.
4. **Funding sources for all the above:** ATF Budget.

Cases

1. **Number of cases ATF Task Force Officer was assigned to:** Eleven – a breakdown of these cases provided below:

    a) Oakland gang member arrested by Ceasefire units with a firearm following his presence at an Oakland shooting. ATF investigation into the suspect led to a federal search warrant at his residence in Las Vegas, NV where numerous firearms and evidence of firearms trafficking were recovered. Defendant has plead guilty in federal court.
    b) Investigation into Oakland gang member trafficking firearms from Texas to Oakland. A federal search warrant at his residence in San Leandro, CA as well as seizure of packages sent by the suspect from Texas led to the recovery of firearms, ammunition, and promethazine syrup which may have been stolen from a pharmacy.
    c) ATF agents traveled to Houston, TX to obtain a federal indictment for firearms possession on a suspect in an Oakland marijuana dispensary homicide.
    d) Investigation into Oakland gang members suspected to be involved in OHAPD shooting resulting in the injury of a juvenile. Federal search warrant at one residence led to the recovery of multiple firearms. Defendant was charged in federal court, case pending. A second related subject was identified as being involved in a Livermore armed robbery as well as a Florida home invasion. State search warrants at an Oakland and Antioch residence resulted in evidence of the crimes. Defendant was arrested for PC211 and pending charges in Florida.
    e) Federal adoption of CHP firearm case led to a federal charge against an Oakland gang member. ATF arrested the suspect at his residence in Antioch where he attempted to flee by ramming law enforcement vehicles and was arrested with a loaded firearm on his person.
    f) Investigation into a gang related homicide in Oakland. One of the involved parties was identified as an Oakland gang member who returned fire during the incident. The defendant is pending federal charges.
    g) ATF investigators assisted OPD homicide with the fire-bombing of a residence which resulted in the death of two people, including a juvenile. Investigation is ongoing.
    h) ATF investigators are assisting CHP with a freeway shooting in Oakland resulting in the death of a juvenile. DNA recovered by ATF lab on fired cartridge cases indicates previously theorized San Francisco gang conflict. Investigation is ongoing.
    i) ATF provided lab assistance for the shooting of retired OPD Captain. DNA recovered by ATF lab on fired cartridge cases matched to one of the suspects. Investigation by ATF in Reno, NV led to evidence of a second suspect with the registered owner of the vehicle used during the shooting.
    j) ATF provided lab assistance for the shooting of a retired law enforcement officer in Oakland. Investigation is ongoing.
    k) ATF agents are currently reviewing all OPD firearm arrests for possible federal prosecution.

2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Firearms investigations, NIBIN/CGIC investigations and Federally adopted State firearm cases.
4. **Number of times the ATF asked OPD to perform/OPD declined to perform:** None.
    a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Note: When criteria is met for federal charging, consideration is provided to ATF through task force or officer.

Operations

1. **Number of times use of undercover officers were approved:** 0
2. **Number of instances where OPD Task Force officer managed informants:** 0
3. **Number of cases involving informants that ATF Task Force Officer worked on:** All cases except adopted cases.
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether ATF Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to ATF Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the ATF Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the ATF Task Force MOU.
2. **Date of last training update:** Continuous Professional Training, June 2021
3. **Frequency with which ATF Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8~~OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force~~.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a

biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No
2. **Whether OPD officer receives SAR information:** No

Command Structure for OPD Task Force Officer

1. **Reports to whom at ATF?** Resident Agent in Charge (RAC) Tommy Ho.
2. **Reports to whom at OPD?** Sergeant Steve Valle and Lieutenant Robert Rosin.

OAKLAND POLICE DEPARTMENT
Drug Enforcement Agency (DEA) Task Force
2021 Annual Report

OPD DEA Taskforce

The DEA State and Local Task Force combines federal leverage and the specialists available to the DEA with state and local officers' investigative talents and detailed knowledge of their jurisdiction to lead drug law enforcement investigations. The DEA shares resources with state and local officers, thereby increasing the investigative possibilities available to all. Participation in DEA Task Forces also allows the DEA to pay for the overtime and investigative expenses of participating police agencies.

Staffing

1. **Number of full and part time Oakland Police Department (OPD officers assigned to DEA Task Force:** One full-time officer
2. **Number of hours worked as DEA Task Force Officer**: Regular 40 hours per week.
3. **Funding source for DEA Task Force Officer salary**: OPD Budget

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone
2. **Surveillance equipment**: GPS Tracker, Wiretap Intercept Equipment (always in possession and managed by DEA).~~None.~~
3. **Clerical/administrative staff hours:** None
4. **Funding sources for all the above:** OPD Budget

Cases

1. **Number of cases DEA Task Force Officer was assigned to:** – case detail breakdown:

   The goal of the Taskforce is to conduct targeted investigations into specific drug trafficking organizations (DTO) and the individuals within the DTOs who are engaged in high level narcotics distribution and trafficking. By conducting these longer federal investigations, the Taskforce is able to ensure entire DTO's are dismantled. Confronting and weakening DTOs closes off specific avenues in which drugs flow into the community. The Taskforce focuses primarily on heroin, methamphetamine, fentanyl, and cocaine trafficking; the Taskforce does not conduct any marijuana investigations.

   Below is a summary of the cases worked on in 2021:

Oakland RO TFG / BB-21-0016

This is an active investigation into the crystal methamphetamine and counterfeit fentanyl pill drug trafficking organization (DTO) operating in and around the Greater Bay Area. The organization was responsible for transporting and trafficking crystal methamphetamine and “M30” fentanyl pills from Mexico into the U.S. from the southern California port of entry. The Oakland Task Force Group to date has arrested seven targets, seized $293,845 in drug proceeds, approximately 10,000 “M30” fentanyl pills, a half kilogram of cocaine, approximately 30 pounds of crystal methamphetamine, and three firearms.

The main target of this investigation was responsible for supplying multiple pound quantities to a distributor who was identified as a member of the violent West Bully 223 street gang, operating in the East Bay area. This investigation was able to thwart the continued growth of the West Bully 223 street gang into a major crystal methamphetamine distributor in the East Bay area. The investigation into other criminal associates and co-conspirators is ongoing.

Oakland RO TFG / BB-21-0056 /

On August 12, 2021, agents from the DEA Oakland Resident Office (ORO) High Intensity Drug Trafficking Area (HIDTA) Task Force Group (TFG), along with the Oakland Alcohol, Tobacco, Firearms, and Explosives (ATF), United States Postal Inspection Service (USPIS), Concord Police Department (CPD), OPD, and the Alameda County Sheriff's Office (ACSO), arrested three suspects. Theses suspects were part of a firearms trafficking organization that was responsible for distributing firearms to violent drug trafficking organizations and known gang members throughout the Bay Area as well as other parts of the United States. As a result of the takedown, agents seized machine guns, privately made firearms (PMFs), silencers, firearms classified as assault weapons/rifles under California State Law, approximately over a thousand rounds of ammunition, high-capacity magazines, unfinished firearm receivers/frames. In total 55 firearms were seized. During the investigation, law enforcement conducted multiple undercover buys resulting in the purchase of 13 firearms and 17 Glock conversion switches, collectively. The undercover purchases netted commercial factory firearms as well as privately made firearms (PMFs), commonly referred to as “ghost guns.” In July of 2021, DEA ORO TFG and ATF, utilized an undercover agent to purchase "M30" fentanyl pills from REMBERT in Concord, CA. Agents later identified the source of supply for those pills, and the investigation into this suspect continues.

Oakland RO TFG/BB-21-0041 /Fentanyl Overdose Death Investigation

On December 5, 2020, the DEA Oakland Resident Office (ORO) Task Force Group (TFG), in partnership with the United States Attorney’s Office (USAO), and their state and local partners, executed the federal arrest warrant of an individual involved in the distribution of fentanyl resulting in death.

This was a six-month long investigation into the Oxycodone and fentanyl drug trafficking activities of the individual. This was a multi-agency investigation. Throughout this investigation, DEA ORO TFG conducted numerous surveillances, interviews, and search warrants to arrest the individual involved. DEA ORO TFG investigators were

also able to utilize technology to identify the individual as the drug trafficker who provided the lethal fentanyl to the overdose victim. Through partnering with their state and local counterparts, DEA ORO TFG was able to link the individual to multiple fentanyl related overdoses. The individual's fatal drug trafficking activities has him facing a mandatory minimum sentence of twenty years in federal prison.

OAKLAND RO TFG/ BB-21-0030

In December of, 2020, the DEA Oakland RO TFG initiated an investigation into the drug trafficking activities of an identified suspect. DEA ORO TFG investigators corroborated intelligence derived from a confidential source (CS) that the suspect was a multi-pound methamphetamine trafficker with ties to Los Angeles and Mexican based drug traffickers. The CS was able to identify locations, vehicles, and methods of operation for the suspect's drug trafficking organization (DTO), which is based in Oakland, CA.

On February 26, 2021, DEA ORO TFG, investigators learned from their CS that the suspect would be traveling to southern California to gain more supply of methamphetamine. OAK-TF-1 investigators then coordinated with California Highway Patrol (CHP) to conduct a traffic stop of the suspect once the vehicle entered the Northern District of California. DEA ORO TFG investigators utilized physical and electronic surveillance on the suspect while on Interstate 5 and 580. Once the suspect entered Alameda County, CHP initiated the stop. As a result of the traffic, CHP discovered 133 pounds of crystal methamphetamine in the suspect's vehicle ready for immediate distribution. The suspect was arrested and charged with federal drug trafficking violations by the United States Attorney's Office (USAO) in the Northern District of California.

Oakland RO TFG / BB-21-0026

In late 2020, the FBI Contra Costa County Safe Streets Task Force (CCCSSTF), DEA RO TFG, and the Concord Police Department (CPD) initiated an Organized Crime Drug Enforcement Task Force (OCDEFT) investigation "Operation Snow Storm" into a Honduran Drug Trafficking Organization (DTO) that distributes large quantities of fentanyl throughout the San Francisco Bay Area. The investigation revealed that several criminal street gang members in Contra Costa County were getting supplied large quantities of fentanyl by the Honduran DTO. A CPD confidential informant identified a high-level member of the DTO. In February 2021, agents learned that the suspect was previously intercepted on a DEA Oakland RO Enforcement Group Title III (T-III) wiretap investigation. In mid-February, DEA ORO TFG, in conjunction with FBI CCCSSTF conducted a buy walk operation with the suspect and purchased approximately a quarter pound of fentanyl. As a result of the aforementioned purchase, law enforcement applied for and received authorization for a federal T-III on the suspect's telephone. During the interception period, law enforcement conducted surveillance and traffic enforcement stops on members of the DTO which resulted in four arrests and approximately one kilogram of fentanyl seized. On May 25, 2021, at the conclusion of the T-III interception period, law enforcement served search warrants at five locations. Approximately 19 kilograms of fentanyl, $37,000 in US Currency, two handguns, and a rifle were seized during the search warrants. The suspect along with seven other criminal associates were arrested on federal drug charges.

Oakland RO TFG Airport Interdiction

Oakland RO TFG have been working in conjunction with the Alameda County Sheriff's Office, Oakland International Airport Insider Threat Task Force. Oakland International Airport is a transit point for drug trafficking and bulk cash smuggling. To date, Oakland RO TFG have seized approximately $900,000 in bulk currency suspected to be drug proceeds or utilized to facilitate drug trafficking.

2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Narcotics investigations and money laundering investigations
4. **Number of times the DEA asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** OPD personnel were assigned in plain clothes or undercover capacity to approximately six investigations.
2. **Number of instances where OPD Task Force officer managed informants:** OPD TFO has three active informants
3. **Number of informant-involved cases in which the OPD DEA Task Force Officer actively participated:** All
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether DEA Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No

Training and Compliance

1. **Description of training given to DEA Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the DEA Task Force follows all OPD policies and has received several police trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the DEA Task Force MOU.
2. **Date of last training update:** Continuous professional training (CPT) in January, 2021
3. **Frequency with which DEA Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8~~OPD will provide~~

~~information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force~~.

2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies, except where DEA policies are more restrictive. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform with State and Federal laws. Going forward, OPD will consult with Office of the City Attorney on a biannual basis.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at DEA?** HIDTA Task Force Group Supervisor Marcelus Ross
2. **Reports to whom at OPD?** Sergeant Valle and Lieutenant Nowak

OAKLAND POLICE DEPARTMENT

FBI Child Exploitation Taskforce
2021 Annual Report

OPD FBI Child Exploitation Taskforce Mission:

The mission of the Child Exploitation and Human Trafficking Task Force (CEHTTF) is to provide a rapid, proactive, and intelligence-driven investigative response to the sexual victimization of children, other crimes against children, and human trafficking within the FBI's jurisdiction; to identify and rescue victims of child exploitation and human trafficking; to reduce the vulnerability of children and adults to sexual exploitation and abuse; to reduce the negative impact of domestic and international parental rights disputes; and to strengthen the capabilities of the FBI and federal, state, local, and international law enforcement through training, intelligence-sharing, technical support, and investigative assistance.

The taskforce follows the following goals and priorities:

1. To rescue victims of sex trafficking that are being exploited on both city streets and through internet crimes.
2. To arrest those individuals who are in violation of prostituted related offenses including 647(a), 647(b), 653.22, and 653.23 P.C, 266 PC, 236.1 PC.
3. To gather intelligence and possibly initiate/pursue investigations on cases involving Human Trafficking or other criminal acts.
4. To assist OPD/FBI investigators on any open/active criminal case. Utilize Federal, state and local resources to locate victims of Human Trafficking and Child Exploitation and look for opportunities to prosecute the subjects Federally.

The defined priority threats that are aligned with the mission of the CEHTTFs are:

1. Child Abductions (Non-Ransom and Ransom)
2. Production/Manufacturing of Child Pornography
3. Sextortion
4. Electronic Groups/Organizations/Enterprises for Profit
5. Travelers/Enticement
6. Traders/Distributors of Child Pornography
7. Interstate Transportation of a Minor with Intent that Minor Engage in Any Illegal Sexual Activity
8. Human Trafficking
9. Child Sex Trafficking
10. Adult Sex Trafficking
11. Forced Labor
12. Domestic Servitude
13. International Parental Kidnapping
14. Possessors of Child Pornography
15. Child Sex Tourism
16. Unlawful Flight to Avoid Prosecution – Parental Kidnapping

17. All other Crimes Against Children and Human Trafficking matters within the FBI's jurisdiction

Staffing

1. **Number of full and part time Oakland Police Department (OPD officers assigned to FBI Task Force:** All Part-Time: (1 Lieutenant, 1 Sergeant and 4 Officers work Part-time Overtime Juvenile Rescue and Internet Crimes Against Children Operations)
2. **Number of hours worked as FBI Task Force Officer**: Each part-time TFO works on average 8 hours a week
3. **Funding source for FBI Task Force Officer salary**: FBI

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone
2. **Surveillance equipment**: Cellebrite machine, GoPro camera
3. **Clerical/administrative staff hours:** None
4. **Clerical/administrative equipment:** laptop computers, hard drives, vehicle usage
5. **Funding sources for all the above:** OPD Budget funds all OPD personnel standard salary and benefits; the FBI in 2021 reimbursed OPD for overtime expenses worked by the federally-deputized OPD members.

Cases

1. **Number of cases FBI Task Force Officer was assigned to:** 12 separate cases; the taskforce conducted over 51 operations in the city of Oakland related to these cases. The results were the following:
    a. One hundred and twenty-nine (129) female adults were arrested for solicitation of prostitution (647(a) and (b) PC, 653.22 PC). They were all offered resources by a combination of several non-profit sexual assault advocate agencies.
    b. One hundred and eleven (111) male adults were arrested for solicitation of prostitution (647(a) and (b) PC, 653.22 PC). The Special Victim Section followed up with "Dear John" letters to applicable residences.
    c. Twenty-two (22) female juveniles were rescued from Human trafficking. They were all provided resources by a combination of several non-profit sexual assault advocate agencies.
    d. Fourteen (14) sex traffickers were arrested and charged with human trafficking (236.1, 266 PC) as a direct result of operations.
    e. The OPD/FBI VICE/Child Exploitation Unit Task Force vetted hundreds of child pornography cyber tips in 2021. This resulted in over 100 search warrants. Five (5) subjects were arrested and prosecuted for Child Pornography (311.11 PC).
    f. The OPD/FBI VICE/Child Exploitation Unit Task Force has provided unmarked vehicles for the use of human trafficking investigations and operations.
    g. In December 2021, The OPD/FBI VICE/Child Exploitation Unit Task Force received a cyber tip regarding an active sexual assault that was documented in child pornography. The OPD/FBI VICE/Child Exploitation Unit Task Force quickly executed a search warrant service which resulted in the following: the scene was located; child pornography was recovered, and the suspect was arrested and

prosecuted. Federal case social workers were also on scene to provide resources to the victim and family members. (Oakland PD RD#21-056098).

a. In April 2020, the OPD/FBI VICE/Child Exploitation Unit Task Force conducted an operation on a "call-out" establishment. Several hours of surveillance were conducted and search warrants were executed.

2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Human Trafficking and Internet Crimes
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** 51 Operations that included undercover officers
2. **Number of instances where OPD Task Force officer managed informants:** None
3. **Number of informant-involved cases in which the OPD FBI Task Force Officer actively participated:** None
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether FBI Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No

Training and Compliance

1. **Description of training given to FBI Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the FBI Task Force follows all OPD policies and has received several police trainings, including but not limited to: Continual Professional Training (CPT), Procedural Justice Training and annual firearms training. OPD VICE/CEU Officers have attended collaborative FBI surveillance training and monthly Innocence Lost meetings. The officer has also reviewed all provisions of the FBI Task Force MOU.
2. **Date of last training update:** FBI taskforce training in January, 2021
3. **Frequency with which FBI Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8~~Release of any of this information would violate California law (832.7), as there is only one OPD officer assigned to this task force~~.

2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at FBI?** Resident Agent in Charge (RAC) Martha Parker
2. **Reports to whom at OPD?** Task Officer reports to Sergeant of the SVS/VICE unit, who is currently Sgt. Marcos Campos. Sergeant reports to the Lieutenant of Special Victims Section is Lt. Alan Yu.

OAKLAND POLICE DEPARTMENT
Federal Bureau of Investigations (FBI)
Violent Crimes / Safe Streets Taskforce
2021 Annual Report

OPD FBI Violent Crimes Taskforce

The OPD FBI Violent Crimes Taskforce which falls under The FBI's Safe Streets initiative, is a collaborative effort to address violence crimes within our community. The task force pursues violent gangs through sustained, proactive, coordinated and intelligence led investigations to obtain prosecutions that will further public safety while reducing harm and law enforcement's footprint.

Staffing

1. **Number of full and part time OPD officers assigned to FBI Task Force:** Two full-time officers.
2. **Number of hours worked as FBI Task Force Officer**: Regular 40 hours per week. However, the current task force officer is often assigned to other OPD operations based on OPD needs and priorities and whether or not there are active investigations.
3. **Funding source for FBI Task Force Officer salary**: OPD Budget.

Other Resources Provided

1. **Communication equipment:** None.
2. **Surveillance equipment:** None.
3. **Clerical/administrative staff hours:** None.
4. **Funding sources for all the above:** OPD Budget.

Cases

1. **Number of cases FBI Task Force Officer was assigned to:** Eleven – a breakdown of these cases provided below:
    a. Two of the cases are ongoing homicide and felony assault cases involving criminal street gangs in the City of Oakland, as well as other Bay Area cities.
    b. There are nine additional ongoing homicide cases in which the FBI Evidence Response Team (ERT) has processed evidence in all of the cases. The cases are all still ongoing; therefore, more detailed information cannot be released currently.
2. **Number of "duty to warn" cases:** N/A
3. **General types of cases:** Homicides and Felony Assault cases involving suspects identified in violent gangs / groups.
4. **Number of times the FBI asked OPD to perform/OPD declined to perform:** None.

a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** Five
2. **Number of instances where OPD Task Force officer managed informants:** None.
3. **Number of informant-involved cases in which the OPD FBI Task Force Officer actively participated:** All cases except adopted cases.
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether FBI Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to FBI Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the FBI Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the FBI Task Force MOU.
2. **Date of last training update:** June 2021
3. **Frequency with which FBI Task Force Officer briefs OPD supervisor on cases:** Weekly

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8~~Release of any of this information would violate California law (832.7), as there are two OPD officers currently assigned to this task force.~~
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at FBI?** Supervisory Agent in Charge (ASAC) Darin Heideman
2. **Reports to whom at OPD?** Lieutenant Frederick Shavies II

OAKLAND POLICE DEPARTMENT
Secret Service
2021 Annual Report

OPD United States Secret Service (USSS) Agreement

OPD and the USSS formalized an agreement related to the USSS Bay Area Identify Theft Strike Force / Electronic Crimes Task Force ("Task Force"). The Memorandum of Understanding (MOU) was signed by both parties in 2009 and articulates rules for reimbursement of participating OPD officers when working on overtime on official Task Force investigations.

Staffing

1. **Number of full and part time OPD officers assigned to USSS Task Force:** One part time officer, who also assists in Criminal Investigations Division (CID) general Crimes.
2. **Number of hours worked as USSS Task Force Officer**: Currently the task force officer spends the majority of his time in the General Crimes office and works with the USSS to assist with active investigations as needed. The assigned officer also uses the USSS task force to assist with digital forensic searches including computers and cell phones.
3. **Funding source for USSS Task Force Officer salary**: OPD Budget – funded by OPD General Purpose Fund.

Other Resources Provided

1. **Communication equipment:** OPD handheld radio, cellular phone.
2. **Surveillance equipment:** Bluetooth skimming devices ~~None~~.
3. **Clerical/administrative staff hours:** None.
4. **Funding sources for all the above:** OPD Budget.

Cases

1. **Number of cases USSS Task Force Officer was assigned to:** This past year the USSS assisted OPD with approximately ten cell phone searches for felony assault. They also assisted OPD with digital forensics related to ATM skimmers and video related to ATM skimmers. The USSS has provided OPD with equipment and training to recognize, detect and locate Bluetooth skimming devices. The USSS also provided OPD with equipment and training to complete cell phone searches.
2. **General types of cases:** Fraud and identity theft investigations
3. **Number of times the USSS asked OPD to perform/OPD declined to perform:** None.
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** None
2. **Number of instances where OPD Task Force officer managed informants:** None.
3. **Number of informant-involved cases in which the OPD USSS Task Force Officer actively participated:** None
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether USSS Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to USSS Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the USSS Task Force follows all OPD policies and has received several trainings, including but not limited to: continual professional training, Procedural Justice Training and annual firearms training. The officer has also reviewed all provisions of the USSS Task Force MOU.
2. **Date of last training:** Sep 2021CPT. Additional USSS Bluetooth skimming device training May 2021
3. **Frequency with which USSS Task Force Officer briefs OPD supervisor on cases:** Daily

Actual and Potential Violations of Local/State Law

~~1.~~ **Number of actual violations** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8. ~~: OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force.~~

~~2.~~1. **Number of potential violations:** Same answer as above.

~~3.~~2. **Actions taken to address actual or potential violations:** The officer follows OPD policies. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform to State and Federal laws.

~~4.~~3. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. Going forward, they will consult on a biannual basis. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at USSS?** Assistant to the Special Agent In Charge (ATSAIC) Danielle Lopez
2. **Reports to whom at OPD?** Sergeant Alexis Nash and Lieutenant Brad Young

OAKLAND POLICE DEPARTMENT
United States Marshals Service (USMS)
2021 Annual Report

OPD USMS Taskforce

The USMS is responsible for enforcing federal court orders and serves as the administrative custodian of all ~~federal~~ warrants until they are executed or dismissed. The USMS also manages warrant information, investigates fugitive matters and executes arrest warrants.

The U.S. Marshals have a long history of providing assistance and expertise to other law enforcement agencies in support of fugitive investigations. The USMS Task Forces does not conduct an independent investigation of possible criminal activity. The USMS only seeks to apprehend individuals with active arrest warrants issued for them related to crimes which have targeted local residents. These crimes include; murder, rape, child molestation, robberies, felony assaults and large scale fraud operations. USMS TFs work by leveraging local police intel as well as well as other data sources (e.g. database searches, open source social media inquiries, and interviews of associates/ and family members).

Staffing

1. **Number of full and part time OPD officers assigned to USMS Task Force:** One full-time officer.
2. **Number of hours worked as USMS Task Force Officer**: Regular 40 hours per week. However, the OPD officer sometimes is asked to assist with OPD operations. The work assignment of this officer is based on OPD needs and priorities and whether there are active investigations.
3. **Funding source for USMS Task Force Officer salary**: OPD General Purpose Fund Budget.

Other Resources Provided

Communication equipment: OPD/USMS radio, cellular phone, laptop.

1. **Surveillance equipment:** None.
2. **Clerical/administrative staff hours:** None.
3. **Funding sources for all the above:** USMS Funds

Cases

1. **Number of cases USMS Task Force Officer was assigned to:** 73; a breakdown of fugitive apprehensions by originating crime type is provided below.

Originating Crime Type Leading To Warrant	Amount
Homicide	28
Robbery	12
Assault	4
Weapons Charges	11
Burglary	3
Rape	4
Aiding Escapee	1
Molesting a Minor	0
Kidnapping	2
Other (e.g. Hit and Run, PAL*, Probation)	8
Total	**73**

*PAL=parolee at large

2. **Number of "duty to warn" cases:** None
3. **General types of cases:** Local, state, and federal criminal arrest warrants.
4. **Number of times USMS asked OPD to perform/OPD declined to perform:** None
   a. **Reason for OPD declination (e.g. insufficient resources, local/state law):** N/A

Operations

1. **Number of times OPD officers were involved in undercover investigations:** None.
2. **Number of instances where OPD Task Force officer managed informants:** None.
3. **Number of informant-involved cases in which the OPD USMS Task Force Officer actively participated:** None.
4. **Number of requests from outside agencies (e.g. ICE) for records or data of OPD:** None.
   a. **Number of such requests that were denied:** N/A
   b. **Reason for denial:** N/A
5. **Whether USMS Task Force Officer was involved in any cases where USPER (U.S. person status) information was collected:** No.

Training and Compliance

1. **Description of training given to USMS Task Force Officer by OPD to ensure compliance with Oakland and California law:** The OPD officer assigned to the USMS Fugitive Task Force follows all OPD policies and procedures, and has received several police trainings, including, but not limited to continued professional training, procedural justice training, and annual firearms training.
2. **Date of last training update:** June 2021 Continuous Professional Training.
3. **Frequency with which USMS Task Force Officer briefs OPD supervisor on cases:** Weekly.

Actual and Potential Violations of Local/State Law

1. **Number of actual violations:** OPD will provide information on law and/or policy violations that are in connection with an officer's task force work, and subject to release under California's Public Records Act, Government Code section 6254 (the "PRA") and/or Cal. Penal Code 832.7. Disclosure of violations not connected to task force work is outside the scope of OMC 9.72. Disclosure of violations beyond those mandated or permitted by statute to be disclosed would violate the prohibition on disclosing personnel or other confidential records set forth in Cal. PC 832.7 & 832.8~~OPD will provide information on violations that are subject to release under California's Public Records Act (the "PRA"), Government Code section 6254. Release of any of violations not covered by the PRA, however, would violate California law (832.7), as there is only one officer assigned to this task force~~.
2. **Number of potential violations:** Same answer as above.
3. **Actions taken to address actual or potential violations:** The Task Force Officer follows OPD policies. USMS Task Force Supervisor meets with OPD VCOC supervisor and commander weekly. OPD leadership consults with the Office of the City Attorney to ensure that all policies conform with State and Federal laws. Going forward OPD will consult with City Attorney on a biannual basis.
4. **Recommendations by OPD to address prevention of future violations:** OPD will continue to consult with the Office of the City Attorney to ensure that personnel continue to follow federal, state, and local laws and policies. OPD will also consult with the Privacy Advisory Commission about any proposed changes.

Suspicious Activity Reports (SARs) and Northern California Regional Intelligence Center (NCRIC)

1. **Whether OPD Task Force Officer submits SARs to NCRIC:** No.
2. **Whether OPD officer receives SAR information:** No.

Command Structure for OPD Task Force Officer

1. **Reports to whom at USMS?** U.S. Marshal Assistant Chief Inspector Gerry Gutierrez.
2. **Reports to whom at OPD?** Sergeant Steve Valle and Lieutenant Robert Rosin.

CITY OF OAKLAND

Annual Report

TO: Privacy Advisory Commission

FROM: Joe DeVries, Chief Privacy Officer

SUBJECT: Impact of Implementing, Tracking and Reporting Ordinance N.O. 13540 C.M.S. - Sanctuary City Contracting and Investment Ordinance

DATE: March 24, 2022

Executive Summary

The Sanctuary City Contracting and Investment Ordinance (Ordinance N.O. 13540 CMS) was adopted by the City Council in June 2019 and requires that by April 1 of each year, the City Administrator shall certify compliance with this ordinance by preparing a written report. By May 1 of each year, the City Administrator shall submit to the Privacy Advisory Commission a written, public report regarding compliance with Sections 2.23.030 and 2.23.040 over the previous calendar year.

At minimum, this report must (1) specify the steps taken to ensure implementation and compliance with Sections 2.23.030 and 2.23.040, (2) disclose process issues, and (3) detail actions taken to cure any process deficiencies. After receiving the recommendation of the Privacy Advisory Commission, if any, the City Administrator shall schedule and submit the written report to the City Council for review and adoption.

Background

The Sanctuary City Contracting and Investment Ordinance prohibits the City from contracting with any person or entity that provides the United States Immigration and Customs Enforcement (ICE), United States Customs and Border Protection (CBP), or Department of Health and Human Services Office of Refugee Resettlement (HHS/ORR) with any "Data Broker", "Extreme Vetting", or "Detention Facilities" services unless the City Council makes a specific determination that no reasonable alternative exists. The ordinance also prohibits the City from investing in any of these companies and requires the City to include notice of these prohibitions in any Requests for Proposals (RFPs), Requests for Qualifications (RFQs), and any construction or other contracting bids.

As is the case in many government entities, the City uses its existing competitive (non-construction services) procurement processes to require compliance with federal, state and local mandates relative to the use of public funds in the purchase of goods and service. For example,

in the late 1980's the City adopted a policy to prohibit doing business with entities that also contract with companies involved in nuclear arms proliferation. In 2013, the City took a stand against contractors doing business with the State of Arizona due to its adoption of legislation that unfairly targeted persons of Hispanic decent in routine traffic stops.

The Sanctuary City Contracting and Investment Ordinance is a response to the recent ICE activity, including its efforts to target Sanctuary Cities with stepped up enforcement efforts and the impact those efforts have had on the Oakland community. There has been strong local interest in these types of ICE raids and deportations both politically and in the media, however, ICE has taken much more drastic steps to gather data on individuals that could ultimately be far more impactful.

Ensuring Compliance

"Schedule I"

The Sanctuary City Contracting and Investment Ordinance (Ordinance N.O. 13540 CMS) is promulgated through "Schedule I" as attached. Any entity wishing to contract with the City of Oakland must self-certify with the Schedule I that they do not have any contracts with ICE, CBP, or HHS/ORR. The Schedule I is submitted along with other contract schedules to the Department of Workplace and Employment Standards (DWES). Staff forward copies of all received Schedule I's to the Chief Privacy Officer. If any contractor cannot self-certify, then a further review of the proposed contract will occur to determine if there are grounds for a waiver.

During the reporting period:

> There was one (1) proposed contractor that was unwilling to sign the Schedule I: Ricoh, U.S.A routinely does business with the DHS including ICE and US Customs. Ricoh, U.S.A. was being considered for a scope of services to scan the Department of Housing and Community Development Rent Adjustment Program's historic case files for the past years. Once scanned, these documents would sit in the City's OnBase document repository. Ricoh, U.S.A was being considered because they had an existing contract with the City of Berkeley to perform a similar scope and it is typically easier for a City to enter into a co-op agreement with another municipality's existing contractor than engaging in an entirely new contract.
>
> The Ricoh, U.S.A. counsel advised the company that it could not sign the Schedule I due to their existing contracts. The CPO advised HCD staff on the ordinance and the options that exist to seek a waiver if qualified, but the staff decided to seek an alternate contractor to perform the work.

Disclosure of Process Issues

There were no negative process issues during this reporting period but as reported above, there was an example of the process working well. The fact that Counsel for a contractor refused to

sing the Schedule I, noting his company's inability to comply suggests the self-reporting process is effective.

Actions Taken to Cure Deficiencies

There were no identified deficiencies in this reporting period to cure.

Investment Prohibitions

The CPO provided the list of prohibited contractors to the Department of Finance to ensure no new investments are made in any of these firms moving forward. As noted during the development of the ordinance, most of the City's investments are in bonds and there are strict guidelines on how a municipality can invest its dollars. Department of Finance agreed to check the list of prohibited entities on a semi-annual basis. The Department reported that in the year 2020, no investments in the prohibited entities were made.

Respectfully submitted,

Joe DeVries,
Chief Privacy Officer

For questions, please contact Joe DeVries, Chief Privacy Officer, at (510) 238-3083.

AMENDED IN ASSEMBLY MARCH 22, 2022

CALIFORNIA LEGISLATURE—2021–22 REGULAR SESSION

ASSEMBLY BILL No. 2336

Introduced by Assembly Members Friedman and Ting

February 16, 2022

An act to amend, repeal, and add Section 70615 of the Government Code, and to amend, repeal, and add Section 9800 of, and to add and repeal Article 3 (commencing with Section 22425) of Chapter 7 of Division 11 of, the Vehicle Code, relating to vehicles.

LEGISLATIVE COUNSEL'S DIGEST

AB 2336, as amended, Friedman. Vehicles: Speed Safety System Pilot Program.

Existing law establishes a basic speed law that prohibits a person from driving a vehicle upon a highway at a speed greater than is reasonable or prudent given the weather, visibility, traffic, and highway conditions, and in no event at a speed that endangers the safety of persons or property.

This bill would authorize, until January 1, 2028, the Cities of Los Angeles, Oakland, San Jose, ~~_____, and _____~~, *and Glendale, one southern California city,* and the City and County of San Francisco, to establish the Speed Safety System Pilot Program if the system meets specified requirements. The bill would require the participating cities or city and county to adopt a Speed Safety System Use Policy and a Speed Safety System Impact Report before implementing the program, and would require the city or city and county to engage in a public information campaign at least 30 days before implementation of the program, including information relating to when the systems would begin detecting violations and where the systems would be utilized.

The bill would require the participating cities or city and county to issue warning notices rather than notices of violations for violations detected within the first 30 calendar days of the program. The bill would require the participating cities or city and county to develop uniform guidelines for, among other things, the processing and storage of confidential information. The bill would designate all photographic, video, or other visual or administrative records made by a system as confidential, and would only authorize public agencies to use and allow access to these records for specified purposes.

This bill would specify that any violation of a speed law recorded by a speed safety system authorized by these provisions would be subject only to the provided civil penalties. The bill would, among other things, provide for the issuance of a notice of violation, an initial review, an administrative hearing, and an appeals process, as specified, for a violation under this program. The bill would require any program created pursuant to these provisions to offer a diversion program for indigent speed safety system violation recipients, as specified. The bill would require a city or city and county participating in the pilot program to submit reports to the Legislature, as specified, to evaluate the speed safety system to determine the system‘s impact on street safety and economic impact on the communities where the system is utilized.

Existing law establishes a $25 filing fee for specified appeals and petitions.

This bill would require a $25 filing fee for an appeal challenging a notice of violation issued as a result of a speed safety system until January 1, 2028.

Existing law establishes that payments for specified charges and penalties, including penalties for offenses relating to the parking of a vehicle, constitute a lien on the vehicle and on any other vehicle owned by the owner of that vehicle.

This bill, until January 1, 2028, would also include as constituting a lien on those vehicles payments for penalties for offenses detected by a speed safety system for which a notice of violation has been served on the owner or recipient of a reissued citation and any delinquent fees added to the penalty.

This bill would make legislative findings and declarations as to the necessity of a special statute for the Cities of Los Angeles, Oakland, San Jose, ~~____, and ____~~, *and Glendale, one southern California city,* and the City and County of San Francisco.

Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all of the following:

(a) Speed is a major factor in traffic collisions that result in fatalities or injuries.

(b) State and local agencies employ a variety of methods to reduce speeding, including traffic engineering, education, and enforcement.

(c) Traffic speed enforcement is critical to efforts in California to reduce factors that contribute to traffic collisions that result in fatalities or injuries.

(d) However, traditional enforcement methods have had a well-documented disparate impact on communities of color, and implicit or explicit racial bias in police traffic stops puts drivers of color at risk.

(e) Additional tools, including speed safety systems, are available to assist cities and the state in addressing excessive speeding and speed-related crashes.

(f) Speed safety systems offer a high rate of detection, and, in conjunction with education and traffic engineering, can significantly reduce speeding, improve traffic safety, and prevent traffic-related fatalities and injuries, including roadway worker fatalities.

(g) Multiple speed safety system programs implemented in other states and cities outside of California have proven successful in reducing speeding and addressing traffic safety concerns.

(h) The Transportation Agency's "CalSTA Report of Findings: AB 2363 Zero Traffic Fatalities Task Force," issued in January 2020, concluded that international and domestic studies show that speed safety systems are an effective countermeasure to speeding

that can deliver meaningful safety improvements, and identified several policy considerations that speed safety system program guidelines could consider.

(i) In a 2017 study, the National Transportation Safety Board (NTSB) analyzed studies of speed safety system programs, and found they offered significant safety improvements in the forms of reduction in mean speeds, reduction in the likelihood of speeding more than 10 miles per hour over the posted speed limit, and reduction in the likelihood that a crash involved a severe injury or fatality. The same study recommended that all states remove obstacles to speed safety system programs to increase the use of this proven approach, and notes that programs should be explicitly authorized by state legislation without operational and location restrictions.

(j) The National Highway Traffic Safety Administration (NHTSA) gives speed safety systems the maximum 5-star effectiveness rating. NHTSA issued speed enforcement camera systems operational guidelines in 2008, and is expected to release revised guidelines in 2021 that should further inform the development of state guidelines.

(k) Speed safety systems can advance equity by improving reliability and fairness in traffic enforcement while making speeding enforcement more predictable, effective, and broadly implemented, all of which helps change driver behavior.

(*l*) Enforcing speed limits using speed safety systems on streets where speeding drivers create dangerous roadway environments is a reliable and cost-effective means to prevent further fatalities and injuries.

SEC. 2. Section 70615 of the Government Code is amended to read:

70615. The fee for filing any of the following appeals to the superior court is twenty-five dollars ($25):

(a) An appeal of a local agency’s decision regarding an administrative fine or penalty under Section 53069.4.

(b) An appeal under Section 40230 of the Vehicle Code of an administrative agency’s decision regarding a parking violation.

(c) An appeal under Section 99582 of the Public Utilities Code of a hearing officer’s determination regarding an administrative penalty for fare evasion or a passenger conduct violation.

(d) A petition under Section 186.35 of the Penal Code challenging a law enforcement agency's inclusion of a person's information in a shared gang database.

(e) An appeal under Section 22428 of the Vehicle Code of a hearing officer's determination regarding a civil penalty for an automated speed violation, as defined in Section 22425 of the Vehicle Code.

(f) This section shall remain in effect only until January 1, 2028, and as of that date is repealed.

SEC. 3. Section 70615 is added to the Government Code, to read:

70615. The fee for filing any of the following appeals to the superior court is twenty-five dollars ($25):

(a) An appeal of a local agency's decision regarding an administrative fine or penalty under Section 53069.4.

(b) An appeal under Section 40230 of the Vehicle Code of an administrative agency's decision regarding a parking violation.

(c) An appeal under Section 99582 of the Public Utilities Code of a hearing officer's determination regarding an administrative penalty for fare evasion or a passenger conduct violation.

(d) A petition under Section 186.35 of the Penal Code challenging a law enforcement agency's inclusion of a person's information in a shared gang database.

(e) This section shall become operative on January 1, 2028.

SEC. 4. Section 9800 of the Vehicle Code is amended to read:

9800. (a) Payments for any of the following, and any interest, penalties, or service fees added thereto, required to register or transfer the registration of a vehicle, constitute a lien on the vehicle on which they are due or which was involved in the offense, and on any other vehicle owned by the owner of that vehicle:

(1) Registration fees.

(2) Transfer fees.

(3) License fees.

(4) Use taxes.

(5) Penalties for offenses relating to the standing or parking of a vehicle for which a notice of parking violation has been served on the owner, and any administrative service fee added to the penalty.

(6) Any court-imposed fine or penalty assessment, and any administrative service fee added thereto, which is subject to collection by the department.

(7) Penalties for offenses detected by a speed safety system, as defined in Section 22425, for which a notice of violation has been served on the owner or recipient of a reissued citation and any delinquent fees added to the penalty.

(b) Notwithstanding subdivision (a), if a person is cited for a foreign registered auxiliary dolly, semitrailer, or trailer having been operated without current year registration or valid California permits or registration, an amount equal to the minimum registration fees or transfer fees, and any penalty added thereto, from the date they became due, shall, by election of the power unit operator, constitute a lien upon the California registered power unit which was pulling the dolly, semitrailer, or trailer. However, this subdivision is not applicable if the citation is issued at a scale operated by the Department of the California Highway Patrol and registration for the vehicle can be issued there immediately upon payment of the fees due.

(c) Every lien arising under this section expires three years from the date the fee, tax, or parking penalty first became due unless the lien is perfected pursuant to subdivision (d).

(d) A lien is perfected when a notice is mailed to the registered and legal owners at the addresses shown in the department's records and the lien is recorded on the electronic vehicle registration records of the department. A perfected lien shall expire five years from the date of perfection.

(e) Employees and members of the Department of the California Highway Patrol assigned to commercial vehicle scale facilities may possess and sell trip permits approved by the Department of Motor Vehicles.

(f) This section shall remain in effect only until January 1, 2028, and as of that date is repealed, unless a later enacted statute that is enacted before January 1, 2028, deletes or extends that date.

SEC. 5. Section 9800 is added to the Vehicle Code, to read:

9800. (a) Payments for any of the following, and any interest, penalties, or service fees added thereto, required to register or transfer the registration of a vehicle, constitute a lien on the vehicle on which they are due or which was involved in the offense, and on any other vehicle owned by the owner of that vehicle:

(1) Registration fees.
(2) Transfer fees.
(3) License fees.
(4) Use taxes.
(5) Penalties for offenses relating to the standing or parking of a vehicle for which a notice of parking violation has been served on the owner, and any administrative service fee added to the penalty.
(6) Any court-imposed fine or penalty assessment, and any administrative service fee added thereto, which is subject to collection by the department.

(b) Notwithstanding subdivision (a), if a person is cited for a foreign registered auxiliary dolly, semitrailer, or trailer having been operated without current year registration or valid California permits or registration, an amount equal to the minimum registration fees or transfer fees, and any penalty added thereto, from the date they became due, shall, by election of the power unit operator, constitute a lien upon the California registered power unit which was pulling the dolly, semitrailer, or trailer. However, this subdivision is not applicable if the citation is issued at a scale operated by the Department of the California Highway Patrol and registration for the vehicle can be issued there immediately upon payment of the fees due.

(c) Every lien arising under this section expires three years from the date the fee, tax, or parking penalty first became due unless the lien is perfected pursuant to subdivision (d).

(d) A lien is perfected when a notice is mailed to the registered and legal owners at the addresses shown in the department's records and the lien is recorded on the electronic vehicle registration records of the department. A perfected lien shall expire five years from the date of perfection.

(e) Employees and members of the Department of the California Highway Patrol assigned to commercial vehicle scale facilities may possess and sell trip permits approved by the Department of Motor Vehicles.

(f) This section shall become operative on January 1, 2028.

SEC. 6. Article 3 (commencing with Section 22425) is added to Chapter 7 of Division 11 of the Vehicle Code, to read:

Article 3. Speed Safety System Pilot Program

22425. (a) As used in this article, the following definitions apply:

(1) "Automated speed violation" means a violation of a speed law detected by a speed safety system operated pursuant to this article.

(2) "Indigent" has the same meaning as defined in subdivision (c) of Section 40220.

(3) "Local department of transportation" means a city or city and county's department of transportation or, if a city or city and county does not have a department of transportation, their administrative division, including, but not limited to, a public works department that administers transportation and traffic matters under this code.

(4) "Speed safety system" or "system" means a fixed or mobile radar or laser system or any other electronic device that utilizes automated equipment to detect a violation of speeding laws and is designed to obtain a clear photograph, video recording, or other visual image of a vehicle license plate.

(b) (1) The Cities of Los Angeles, Oakland, San Jose, ~~_____~~, ~~and _____~~, *and Glendale, one southern California city,* and the City and County of San Francisco, may establish a program utilizing a speed safety system for speed enforcement, to be operated by a local department of transportation, in the following areas:

(A) On a street meeting the standards of a safety corridor under Section 22358.7.

(B) On a street a local authority has determined to have had a high number of incidents for motor vehicle speed contests or motor vehicle exhibitions of speed.

(C) School zones, subject to subdivision (d).

(2) A municipality operating a speed safety system pilot program under this article may have speed safety systems operational on no more than 15 percent of the municipality's streets at any time during the pilot program.

(3) (A) A municipality operating a speed safety pilot program under this article may have the following number of speed safety systems operational at any time during the pilot program:

(i) For a jurisdiction with a population over 3,000,000, no more than 125 systems.

(ii) For a jurisdiction with a population between 800,000 and 3,000,000, inclusive, no more than 33 systems.

(iii) For a jurisdiction with a population of 300,000 up to 800,000, no more than 18 systems.

(iv) For a jurisdiction with a population of less than 300,000, no more than nine systems.

(B) For purposes of this paragraph, a "speed safety system" may include up to two fixed or mobile radar or laser systems at the same location in order to detect speed violations on two-way or multidirectional streets.

(c) The Speed Safety System Pilot Program shall not be operated on any California state route, including all freeways and expressways, United States Highway, Interstate Highway or any public road in an unincorporated county where the Commissioner of the California Highway Patrol has full responsibility and primary jurisdiction for the administration and enforcement of the laws, and for the investigation of traffic accidents, pursuant to Section 2400.

(d) If a school zone has a posted speed limit of 30 miles per hour or higher when children are not present, a city or city and county may operate a speed safety system two hours before the regular school session begins and two hours after regular school session concludes.

(e) A speed safety system for speed limit enforcement may be utilized pursuant to subdivision (b) if the program meets all of the following requirements:

(1) Clearly identifies the presence of the speed safety system by signs stating "Photo Enforced," along with the posted speed limit within 500 feet of the system. The signs shall be visible to traffic traveling on the street from the direction of travel for which the system is utilized, and shall be posted at all locations as may be determined necessary by the Department of Transportation through collaboration with the California Traffic Control Devices Committee.

(2) Identifies the streets or portions of streets that have been approved for enforcement using a speed safety system and the hours of enforcement on the municipality's internet website, which shall be updated whenever the municipality changes locations of enforcement.

(3) Ensures that the speed safety system is regularly inspected and certifies that the system is installed and operating properly. Each camera unit shall be calibrated in accordance with the manufacturer's instructions, and at least once per year by an independent calibration laboratory. Documentation of the regular inspection, operation, and calibration of the system shall be retained until the date on which the system has been permanently removed from use.

(4) Utilizes fixed or mobile speed safety systems that provide real-time notification when violations are detected.

(f) Prior to enforcing speed laws utilizing speed safety systems, the city or city and county shall do both of the following:

(1) Administer a public information campaign for at least 30 calendar days prior to the commencement of the program, which shall include public announcements in major media outlets and press releases. The public information campaign shall include the draft Speed Safety System Use Policy pursuant to subdivision (g), the Speed Safety System Impact Report pursuant to subdivision (h), information on when systems will begin detecting violations, the streets, or portions of streets, where systems will be utilized, and the city's internet website, where additional information about the program can be obtained. Notwithstanding the above, no further public announcement by the municipality shall be required for additional systems that may be added to the program.

(2) Issue warning notices rather than notices of violation for violations detected by the speed safety systems during the first 30 calendar days of enforcement under the program. If additional systems are utilized on additional streets after the initial program implementation, the city or city and county shall issue warning notices rather than notices of violation for violations detected by the new speed safety systems during the first 30 calendar days of enforcement for the additional streets added to the program.

(g) The local governing body shall adopt a Speed Safety System Use Policy before entering into an agreement regarding a speed safety system, purchasing or leasing equipment for a program, or implementing a program. The Speed Safety System Use Policy shall include the specific purpose for the system, the uses that are authorized, the rules and processes required prior to that use, and the uses that are prohibited. The policy shall include the data or information that can be collected by the speed safety system and

the individuals who can access or use the collected information, and the rules and processes related to the access or use of the information. The policy shall also include provisions for protecting data from unauthorized access, data retention, public access, third-party data sharing, training, auditing, and oversight to ensure compliance with the Speed Safety System Use Policy. The Speed Safety System Use Policy shall be made available for public review, including, but not limited to, by posting it on the local governing body's internet website at least 30 calendar days prior to adoption by the local governing body.

(h) (1) The local governing body also shall approve a Speed Safety System Impact Report prior to implementing a program. The Speed Safety System Impact Report shall include all of the following information:

(A) Assessment of potential impact of the speed safety system on civil liberties and civil rights and any plans to safeguard those public rights.

(B) Description of the speed safety system and how it works.

(C) Fiscal costs for the speed safety system, including program establishment costs, ongoing costs, and program funding.

(D) If potential deployment locations of systems are predominantly in low-income neighborhoods, a determination of why these locations experience high fatality and injury collisions due to unsafe speed.

(E) Locations where the system may be deployed and traffic data for these locations.

(F) Proposed purpose of the speed safety system.

(2) The Speed Safety System Impact Report shall be made available for public review at least 30 calendar days prior to adoption by the governing body.

(3) The local governing body shall consult and work collaboratively with relevant local stakeholder organizations, including racial equity, privacy protection, and economic justice groups, in developing the Speed Safety System Use Policy and Speed Safety System Impact Report.

(i) The municipality shall develop uniform guidelines for both of the following:

(1) The screening and issuing of notices of violation.

(2) The processing and storage of confidential information and procedures to ensure compliance with confidentiality requirements.

(j) Notices of violation issued pursuant to this section shall include a clear photograph, video recording, or other visual image of the license plate and rear of the vehicle only, the Vehicle Code violation, the camera location, and the date and time when the violation occurred. Notices of violation shall exclude images of the rear window area of the vehicle.

(k) The photographic, video, or other visual evidence stored by a speed safety system does not constitute an out-of-court hearsay statement by a declarant under Division 10 (commencing with Section 1200) of the Evidence Code.

(*l*) (1) Notwithstanding Sections 6253 and 6262 of the Government Code, or any other law, photographic, video, or other visual or administrative records made by a system shall be confidential. Public agencies shall use and allow access to these records only for the purposes authorized by this article or to assess the impacts of the system.

(2) Confidential information obtained from the Department of Motor Vehicles for the administration of speed safety systems and enforcement of this article shall be held confidential, and shall not be used for any other purpose.

(3) Except for court records described in Section 68152 of the Government Code, or as provided in paragraph (4), the confidential records and evidence described in paragraphs (1) and (2) may be retained for up to 60 days after final disposition of the notice of violation. The municipality may adopt a retention period of less than 60 days in the Speed Safety System Use Policy. Administrative records described in paragraph (1) may be retained for up to 120 days after final disposition of the notice of violation. Notwithstanding any other law, the confidential records and evidence shall be destroyed in a manner that maintains the confidentiality of any person included in the record or evidence.

(4) Notwithstanding Section 26202.6 of the Government Code, photographic, video, or other visual evidence that is obtained from a speed safety system that does not contain evidence of a speeding violation shall be destroyed within five business days after the evidence was first obtained. The use of facial recognition technology in conjunction with a speed safety system shall be prohibited.

(5) Information collected and maintained by a municipality using a speed safety system shall only be used to administer an

program, and shall not be disclosed to any other persons, including, but not limited to, any other state or federal government agency or official for any other purpose, except as required by state or federal law, court order, or in response to a subpoena in an individual case or proceeding.

(m) Notwithstanding subdivision (*l*), the registered owner or an individual identified by the registered owner as the driver of the vehicle at the time of the alleged violation shall be permitted to review the photographic, video, or visual evidence of the alleged violation.

(n) A contract between the municipality and a manufacturer or supplier of speed safety systems shall allow the local authority to purchase materials, lease equipment, and contract for processing services from the manufacturer or supplier based on the services rendered on a monthly schedule or another schedule agreed upon by the municipality and contractor. The contract shall not include provisions for payment or compensation based on the number of notices of violation issued by a designated municipal employee, or as a percentage of revenue generated, from the use of the system. The contract shall include a provision that all data collected from the speed safety systems is confidential, and shall prohibit the manufacturer or supplier of speed safety systems from sharing, repurposing, or monetizing collected data, except as specifically authorized in this article. The municipality shall oversee and maintain control over all enforcement activities, including the determination of when a notice of violation should be issued.

(o) Notwithstanding subdivision (n), a municipality may contract with a vendor for the processing of notices of violation after a designated municipal employee has issued a notice of violation. The vendor shall be a separate legal and corporate entity from, and unrelated or affiliated in any manner with, the manufacturer or supplier of speed safety systems used by the municipality. Any contract between the municipality and a vendor to provide processing services may include a provision for the payment of compensation based on the number of notices of violation processed by the vendor.

(p) (1) A speed safety system shall no longer be operated on any given street if within the first 18 months of installation of a system, at least one of the following thresholds has not been met:

(A) Percentage of automated speed violations decreased by at least 25 percent.

(B) Percentage of violators who received two or more violations decreased by at least 50 percent.

(2) This subdivision does not apply if a city or city and county adds traffic-calming measures to the street. "Traffic-calming measures" include, but are not limited to:

(A) Bicycle lanes.

(B) Chicanes.

(C) Chokers.

(D) Curb extensions.

(E) Median islands.

(F) Raised crosswalks.

(G) Road diets.

(H) Roundabouts.

(I) Speed humps or speed tables.

(J) Traffic circles.

(3) A city or city and county may continue to operate a speed safety system with a fixed or mobile vehicle speed feedback sign while traffic-calming measures are being planned or constructed, but shall halt their use if construction has not begun within two years.

(4) If the percentage of violations has not decreased by the metrics identified pursuant to paragraph (1) within one year after traffic-calming measures have completed construction, a city or county shall either construct additional traffic-calming measures or cease operation of the system on that street.

22426. (a) Notwithstanding any other law, a violation of Section 22350, or any other speed law pursuant to this chapter that is recorded by a speed safety system authorized pursuant to Section 22425 shall be subject only to a civil penalty, as provided in subdivision (c), and shall not result in the department suspending or revoking the privilege of a violator to drive a motor vehicle or in a violation point being assessed against the violator.

(b) The speed safety system shall capture images of the rear license plate of vehicles that are traveling 11 miles per hour or more over the posted speed limit and notices of violation shall only be issued to vehicles based on that evidence.

(c) A civil penalty shall be assessed as follows:

(1) Fifty dollars ($50) for a speed violation from 11 up to 15 miles per hour over the posted speed limit.

(2) One hundred dollars ($100) for a speed violation from 16 up to ~~26~~ *25* miles per hour over the posted speed limit.

(3) Two hundred dollars ($200) for a speed violation ~~from 25 up to 100~~ *of 26* miles per hour *or more* over the posted speed ~~limit.~~ *limit, unless paragraph (4) applies.*

(4) Five hundred dollars ($500) for ~~a speed violation~~ *traveling at a speed of* 100 miles per hour or ~~greater over the posted speed limit.~~ *greater.*

(d) A civil penalty shall not be assessed against an authorized emergency vehicle.

(e) The written notice of violation shall be issued to the registered owner of the vehicle within 15 calendar days of the date of the violation. The notice of violation shall include all of the following information:

(1) The violation, including reference to the speed law that was violated.

(2) The date, approximate time, and location where the violation occurred.

(3) The vehicle license number and the name and address of the registered owner of the vehicle.

(4) A statement that payment is required to be made no later than 30 calendar days from the date of mailing of the notice of violation, or that the violation may be contested pursuant to Section 22427.

(5) The amount of the civil penalty due for that violation and the procedures for the registered owner, lessee, or rentee to pay the civil penalty or to contest the notice of violation.

(6) An affidavit of nonliability, and information of what constitutes nonliability, information as to the effect of executing the affidavit, and instructions for returning the affidavit to the processing agency. If the affidavit of nonliability is returned to the processing agency within 30 calendar days of the mailing of the notice of violation, together with proof of a written lease or rental agreement between a bona fide rental or leasing company and its customer that identifies the rentee or lessee, the processing agency shall serve or mail a notice of violation to the rentee or lessee identified in the affidavit of nonliability.

(f) Mobile radar or laser systems shall not be used until at least two years after the installation of the first fixed radar or laser system.

(g) (1) Revenues derived from any program utilizing a speed safety system for speed limit enforcement shall first be used to recover program costs. Program costs include, but are not limited to, the construction of traffic calming measures for the purposes of complying with subdivision (p) of Section 22425, the installation of speed safety systems, the adjudication of violations, and reporting requirements as specified in this section.

(2) Jurisdictions shall maintain their existing commitment of local funds for traffic-calming measures in order to remain authorized to participate in the pilot program, and shall annually expend not less than the annual average of expenditures for traffic-calming measures during the 2016–17, 2017–18, and 2018–19 fiscal years. For purposes of this subdivision, in calculating average expenditures on traffic-calming measures, restricted funds that may not be available on an ongoing basis, including those from voter-approved bond issuances or tax measures, shall not be included. Any excess revenue shall be used for traffic calming measures within three years. If traffic-calming measures are not planned or constructed after the third year, excess revenue shall revert to the Active Transportation Program established pursuant to Chapter 8 (commencing with Section 2380) of the Streets and Highways Code, to be allocated by the California Transportation Commission pursuant to Section 2381 of the Streets and Highways Code.

22427. (a) For a period of 30 calendar days from the mailing of a notice of violation, a person may request an initial review of the notice by the issuing agency. The request may be made by telephone, in writing, electronically, or in person. There shall be no charge for this review. If, following the initial review, the issuing agency is satisfied that the violation did not occur, or that extenuating circumstances make dismissal of the notice of violation appropriate in the interest of justice, the issuing agency shall cancel the notice of violation. The issuing agency shall advise the processing agency, if any, of the cancellation. The issuing agency or the processing agency shall mail the results of the initial review to the person contesting the notice, and, if cancellation of the notice does not occur following that review, include a reason for that

denial, notification of the ability to request an administrative hearing, and notice of the procedure adopted pursuant to paragraph (2) of subdivision (b) for waiving prepayment of the civil penalty based upon an inability to pay.

(b) (1) If the person contesting the notice of violation is dissatisfied with the results of the initial review, the person may, no later than 21 calendar days following the mailing of the results of the issuing agency's initial review, request an administrative hearing of the violation. The request may be made by telephone, in writing, electronically, or in person.

(2) The person requesting an administrative hearing shall pay the amount of the civil penalty to the processing agency. The issuing agency shall adopt a written procedure to allow a person to request an administrative hearing without payment of the civil penalty upon satisfactory proof of an inability to pay the amount due.

(3) The administrative hearing shall be held within 90 calendar days following the receipt of a request for an administrative hearing. The person requesting the hearing may request one continuance, not to exceed 21 calendar days.

(c) The administrative hearing process shall include all of the following:

(1) The person requesting a hearing shall have the choice of a hearing by mail, video conference, or in person. An in-person hearing shall be conducted within the jurisdiction of the issuing agency.

(2) If the person requesting a hearing is a minor, that person shall be permitted to appear at a hearing or admit responsibility for the automated speed violation without the appointment of a guardian. The processing agency may proceed against the minor in the same manner as against an adult.

(3) The administrative hearing shall be conducted in accordance with written procedures established by the issuing agency and approved by the governing body or chief executive officer of the issuing agency. The hearing shall provide an independent, objective, fair, and impartial review of contested automated speed violations.

(4) (A) The issuing agency's governing body or chief executive officer shall appoint or contract with qualified independent examiners or administrative hearing providers that employ qualified

independent examiners to conduct the administrative hearings. Examiners shall demonstrate the qualifications, training, and objectivity necessary to conduct a fair and impartial review. The examiner shall be separate and independent from the notice of violation collection or processing function. An examiner's continued employment, performance evaluation, compensation, and benefits shall not, directly or indirectly, be linked to the amount of civil penalties collected by the examiner or the number or percentage of violations upheld by the examiner.

(B) (i) Examiners shall have a minimum of 20 hours of training. The examiner is responsible for the costs of the training. The issuing agency may reimburse the examiner for those costs. Training may be provided through any of the following:

(I) An accredited college or university.

(II) A program conducted by the Commission on Peace Officer Standards and Training.

(III) A program conducted by the American Arbitration Association or a similar organization.

(IV) Any program approved by the governing body or chief executive officer of the issuing agency, including a program developed and provided by, or for, the agency.

(ii) Training programs may include topics relevant to the administrative hearing, including, but not limited to, applicable laws and regulations, enforcement procedures, due process, evaluation of evidence, hearing procedures, and effective oral and written communication. Upon the approval of the governing body or chief executive officer of the issuing agency, up to 12 hours of relevant experience may be substituted for up to 12 hours of training. Up to eight hours of the training requirements described in this subparagraph may be credited to an individual, at the discretion of the governing body or chief executive officer of the issuing agency, based upon training programs or courses described in this subparagraph that the individual attended within the last five years.

(5) The designated municipal employee who issues a notice of violation shall not be required to participate in an administrative hearing. The issuing agency shall not be required to produce any evidence other than, in proper form, the notice of violation or copy thereof, including the photograph, video, or other visual image of the vehicle's license plate, and information received from the

Department of Motor Vehicles identifying the registered owner of the vehicle. The documentation in proper form shall be prima facie evidence of the violation.

(6) The examiner's final decision following the administrative hearing may be personally delivered to the person by the examiner or sent by first-class mail.

(7) Following a determination by the examiner that a person has committed the violation, the examiner may, consistent with the written guidelines established by the issuing agency, allow payment of the civil penalty in installments, or an issuing agency may allow for deferred payment or payments in installments, if the person provides evidence satisfactory to the examiner or the issuing agency, as the case may be, of an inability to pay the civil penalty in full. If authorized by the governing body of the issuing agency, the examiner may permit the performance of community service in lieu of payment of the civil penalty.

(8) If a notice of violation is dismissed following an administrative hearing, any civil penalty, if paid, shall be refunded by the issuing agency within 30 days.

22428. (a) Within 30 days after personal delivery or mailing of the final decision described in subdivision (c) of Section 22427, the contestant may seek review by filing an appeal to the superior court, where the case shall be heard de novo, except that the contents of the processing agency's file in the case on appeal shall be received in evidence. A copy of the notice of violation shall be admitted into evidence as prima facie evidence of the facts stated in the notice. A copy of the notice of appeal shall be served in person or by first-class mail upon the processing agency by the contestant. For purposes of computing the 30-day period, Section 1013 of the Code of Civil Procedure shall be applicable. A proceeding under this subdivision is a limited civil case.

(b) The fee for filing the notice of appeal shall be as provided in Section 70615 of the Government Code. The court shall request that the issuing agency's file on the case be forwarded to the court, to be received within 15 calendar days of the request. The court shall notify the contestant of the appearance date by mail or personal delivery. The court shall retain the fee under Section 70615 of the Government Code regardless of the outcome of the appeal. If the appellant prevails, this fee and any payment of the

civil penalty shall be promptly refunded by the issuing agency in accordance with the judgment of the court.

(c) The conduct of the hearing on appeal under this section is a subordinate judicial duty that may be performed by a commissioner or other subordinate judicial officer at the direction of the presiding judge of the court.

(d) If a notice of appeal of the examiner's decision is not filed within the period set forth in subdivision (a), the decision shall be deemed final.

(e) If the civil penalty has not been paid and the decision is adverse to the contestant, the processing agency may, promptly after the decision becomes final, proceed to collect the civil penalty under Section 22426.

22429. (a) A city or city and county shall offer a diversion program for indigent speed safety system violation recipients, to perform community service in lieu of paying the penalty for an automated speed system violation.

(b) A city or city and county shall offer the ability for indigent speed safety system violation recipients to pay applicable fines and penalties over a period of time under a payment plan with monthly installments of no more than twenty-five dollars ($25) and shall limit the processing fee to participate in a payment plan to five dollars ($5) or less.

(c) Notwithstanding subdivisions (a) and (b), a city or city and county shall reduce the applicable fines and penalties by 80 percent for indigent persons, and by 50 percent for individuals 200 percent above the federal poverty level.

22430. A city or city and county shall each develop and submit to their respective governing body a Speed Safety System Report, two years after initial implementation of the program and at the end of the pilot program that includes all of the following information:

(a) A description of how the speed safety system was used.

(b) Whether and how often any system data was shared with outside entities, the name of any recipient entity, the type or types of data disclosed, and the legal reason for the disclosure.

(c) A summary of any community complaints or concerns about the speed safety system.

(d) Results of any internal audits, information about any violations of the Speed Safety System Use Policy, and any actions taken in response.

(e) Information regarding the impact the speed safety system has had on the streets where the speed safety system was deployed.

(f) A summary of any public record act requests.

(g) A list of system locations that did not meet the threshold for continuance of a program pursuant to paragraph (1) of subdivision (p) of Section 22425, and whether further traffic-calming measures are in planning or construction, or there is a decision to halt operation of the program in those locations.

22431. Any city or city and county that used speed safety systems shall, on or before March 1 of the fifth year in which the system has been implemented, submit to the transportation committees of the Legislature an evaluation of the speed safety system in their respective jurisdictions to determine the system's impact on street safety and the system's economic impact on the communities where the system is utilized. The report shall be made available on the internet websites of the respective jurisdictions and shall include all of the following information:

(a) Data, before and after implementation of the system, on the number and proportion of vehicles speeding from 11 to 19 miles per hour over the legal speed limit, inclusive, from 20 to 29 miles per hour over the legal speed limit, inclusive, from 30 to 39 miles per hour over the legal speed limit, inclusive, and every additional 10 miles per hour increment thereafter on a street or portion of a street in which an system is used to enforce speed limits. To the extent feasible, the data should be collected at the same time of day, day of week, and location.

(b) The number of notices of violation issued under the program by month and year, the corridors or locations where violations occurred, and the number of vehicles with two or more violations in a monthly period and a yearly period.

(c) Data, before and after implementation of the system, on the number of traffic collisions that occurred where speed safety systems are used, relative to citywide data, and the transportation mode of the parties involved. The data on traffic collisions shall be categorized by injury severity, such as property damage only, complaint of pain, other visible injury, or severe or fatal injury.

(d) The number of violations paid, the number of delinquent violations, and the number of violations for which an initial review is requested. For the violations in which an initial review was requested, the report shall indicate the number of violations that went to initial review, administrative hearing, and de novo hearing, the number of notices that were dismissed at each level of review, and the number of notices that were not dismissed after each level of review.

(e) The costs associated with implementation and operation of the speed safety systems, and revenues collected by each jurisdiction.

(f) A racial and economic equity impact analysis, developed in collaboration with local racial justice and economic equity stakeholder groups.

22432. This article shall remain in effect only until January 1, 2028, and as of that date is repealed.

SEC. 7. The Legislature finds and declares that a special statute is necessary and that a general statute cannot be made applicable within the meaning of Section 16 of Article IV of the California Constitution because of the unique circumstances with traffic speed enforcement in the Cities of Los Angeles, Oakland, San Jose, ~~_____,~~ ~~and _____~~, *and Glendale, one southern California city,* and the City and County of San Francisco.

SEC. 8. The Legislature finds and declares that Section 6 of this act, which adds Section 22425 to the Vehicle Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

To protect the privacy interests of persons who are issued notices of violation under a speed safety systems pilot program, the Legislature finds and declares that the photographic, video, or other visual or administrative records generated by the program shall be confidential, and shall be made available only to alleged violators and to governmental agencies solely for the purpose of

enforcing these violations and assessing the impact of the use of speed safety systems, as required by this act.

O

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:
CrimeView Product Suite

A. Description: The CrimeView Product Suite and Function

The CentralSquare[1] geospatial CrimeView product suite has been the core technology resource for the Oakland Police Department (OPD) crime analysts since 2008. OPD law enforcement personnel and crime analysts have been using CrimeView software for several years. The CrimeView product suite comprises three geospatial applications.

1. CrimeView Desktop is a specialized application for dedicated crime analysts. With this unique software application, analysts can connect to the City's Geographic Information Systems (GIS) ESRI (GIS software vendor) enterprise software ArcGIS (see ***Attachment A*** for the Desktop Operating Manual). Integration with the City's ArcGIS software is a feature that only CentralSquare offers. The connection of CrimeView Desktop with the City's GIS system lets analysts create detailed geographical reports. With this information, police commanders and investigators can make informed, data-driven decisions on how best to reduce crime in the city.

2. CrimeView Analytics is an upgrade from the current CrimeView Dashboard product[2]. This browser-based application connects with OPD incident data to let police officers and commanders access useful geographical data visualizations. CrimeView Analytics lets OPD personnel view data by crime or penal code, by police beat or area, and by time of day. These data views provide useful crime pattern analysis for officers, OPD commanders, and crime analysts. The CrimeView Analytics upgrade will allow for greater flexibility within the application's paradigm, including support for on-demand queries, scheduled report generation, threshold alerting, and density maps.

3. Crimemapping.com is the public facing application, providing the public with a map-based view of crime incidents in the City of Oakland[3]. This application complements the City's already existing IDT-based

[1] CrimeView was originally created by the Omega Group, which was later purchased by Tritech. TriTech merged with Central Square in Sept. 2018.
[2] An online manual for the CrimeView Analytics can be found here: https://crimeviewanalytics.csqr.cloud/resources/crimeview/userguide/Content/Overview%20of%20CrimeView.htm

[3] An online manual for the CrimeMapping can be found here: https://www.crimemapping.com/help

CrimeWatch open-data initiative.

B. Proposed Purpose

CentralSquare's CrimeView product suite (see ***Attachment B*** CrimeView Analytics Overview) provides three core services for OPD: 1) a specialized license-based desktop application for crime analysts; 2) a web-based application for OPD personnel; and 3) a public facing geospatial application for the public.

The CrimeView product suite provides geospatial and temporal information, which in turn supports crime analysts' efforts to provide relevant intelligence to OPD's law enforcement personnel This precision data lets commanders and officers target environments where their intervention results in the most positive impact possible. This data-driven approach to command decision making supports OPD's intelligence-led and precision-based policing initiatives. OPD's data-driven and intelligence-led policing initiatives allow OPD to minimize the impact of policing across Oakland communities – while still providing police services.

1. CrimeView Desktop – This application is an extension to ESRI's ArcGIS application. This extension lets crime analysts map OPD's crime incident data and use ArcGIS's spatial analysis tools to create detailed reports for OPD officers, investigators, and commanders. This application is only used by crime analysts and requires an advanced working knowledge of ESRI's ArcGIS application and its geospatial analysis tools.
   The generated reports provide critical information about crime from a geospatial perspective in an easy-to-view format, including temporal information, that assists in resource deployment and other operational decisions. This application is the workhorse of OPD's Crime Analysis Section, letting analysts provide a depth and breadth of work that would otherwise be impossible. CrimeView Desktop streamlines the geospatial process, saving a huge number of staff hours. This lets analysts use their training and experience to interpret the results and provide critical analytical commentary to support the program's findings.

2. CrimeView Analytics – This web-based application lets police officers and commanders access useful geographical data visualizations by crime or penal code, by police beat or area, and by time of day. These data views provide useful crime pattern analysis for officers, when a detailed, hand-built report may not be necessary. By giving OPD personnel the ability to perform simple visualizations on their own, they are empowered to make operational decisions when a dedicated crime analyst may not be available. Additionally, snapshot views can be created by crime analysts, to give executive team members and area captains a high-level view of crime any time of the day.
3. Crimemapping.com – This application is the public-facing portion of the product suite. It provides a simple map-based view of crime. It is intended for general use, and therefore data is anonymized to protect the privacy of crime victims and the integrity of ongoing investigations.

Members of the public can also see other jurisdictions that subscribe to the service and create their own alerts for areas they are concerned about. As mentioned previously, this application complements the City's already existing IDT-based CrimeWatch open data initiative.

C. Locations where, and situations in which, the CentralSquare CrimeView product suite may be deployed or used.

The CrimeView product suite is separated into three different applications, so that different groups have access only to the application they are authorized to use.

1. CrimeView Desktop – Only crime analysts can use this application, which is an extension to ESRI's ArcGIS desktop mapping application. This license-based software is installed only on devices solely used by crime analysts. These computers are secured within the Police Administration Building (PAB) on floors and in sections that can only be accessed by an employee's keycard. Each employee's network profile is secured, and only authorized employees can access and use CrimeView Desktop.

2. CrimeView Analytics – Only OPD personnel can access this application. OPD personnel are individuals who have undergone a complete background check and have fulfilled the California Department of Justice requirements for using computers on the OPD network. These requirements include, but are not limited to, a written test taken every two years on accessing the California Law Enforcement Telecommunication System (CLETS) as well as a state-mandated four-hour in-person training covering the handling and release of confidential information. Everyone using CrimeView Analytics must have his or her own individual login and password; logins cannot be shared. The manager of the Crime Analysis Section personally approves and maintains the list of approved users. Information in CrimeView Analytics is considered internal confidential information, and it cannot be shared with the public – information in Analytics contains information that could compromise, if released, victim privacy and safety as well as ongoing investigations.

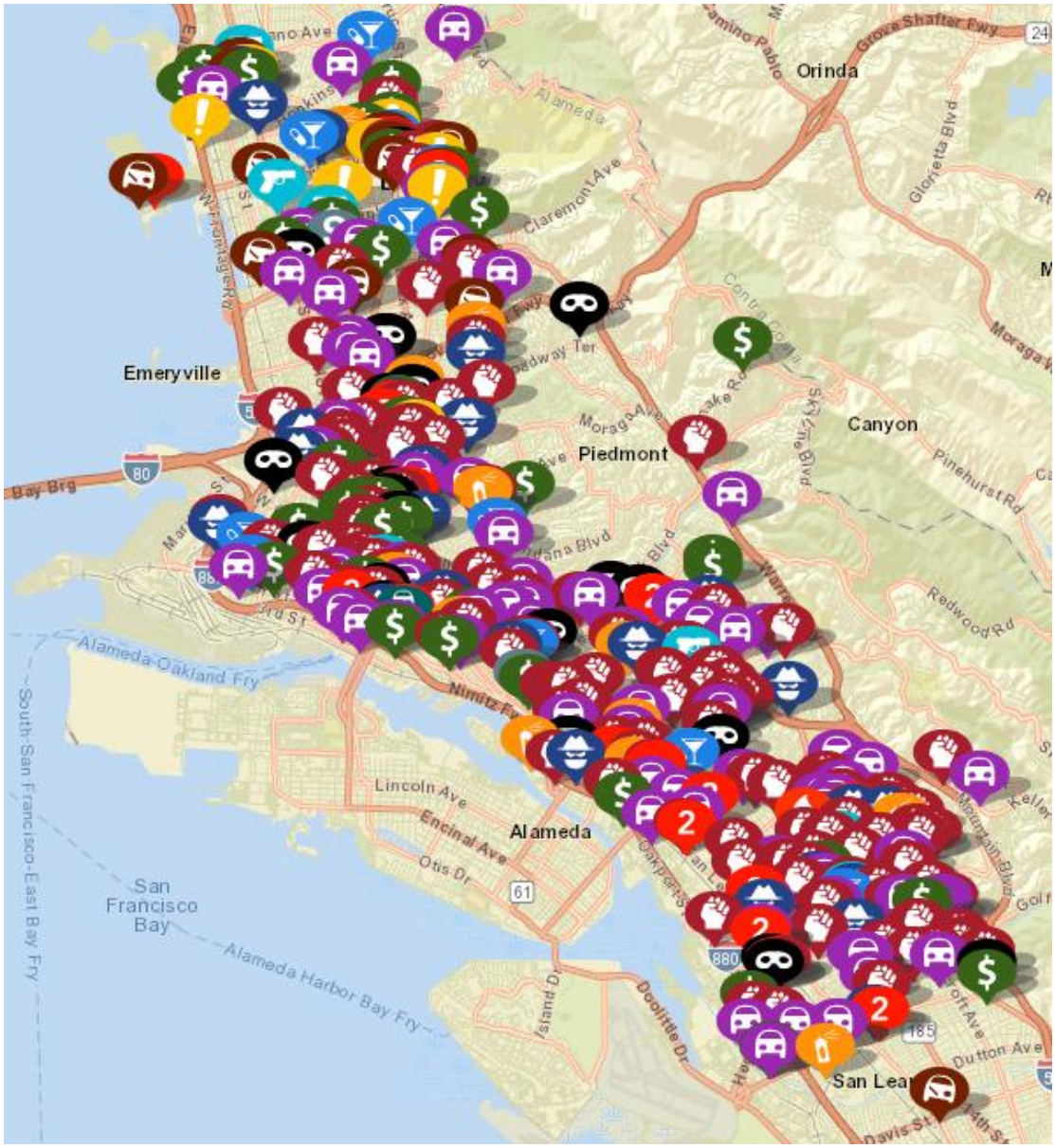
3. Crimemapping.com – Any member of the public can access this application. The information displayed in this geospatial application has been formatted to allow the public an anonymized view of crime in Oakland, which protecting the privacy and safety of victims and the integrity of ongoing investigations.

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year. OPD utilizes CrimeView Desktop and CrimeView Analytics to better strategize ways to confront the high levels of crime illustrated in this data table. These crimes occur throughout the City although there are parts of the city that unfortunately see much higher concentrations of violent crime. The CrimeView Desktop and CrimeView Analytics products help OPD Command to best leverage limited resources to confront areas where crime is most concentrated.

Part 1 Crimes *All totals include attempts except homicides*	01-01-2020 through 12-31-2020	01-01-2021 through 12-31-2021	Year-to-Date % Change 2020 vs. 2021	3-Year Year-to-Date Average	YTD 2021 vs. 3-Year YTD Average
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Figure 1 below is a screenshot taken from CrimeMapping.com on March 21, 2022. The Central Square product suite includes this public-facing website. Members of the public can use this website to view crime maps and filter by crime type and location area within the City.

Figure 1: Oakland Crimemapping.com Screenshot



D. Impact

The aggregation of data will always cause concern of impacts to public privacy. Data used in CentralSquare's CrimeView product suite originates solely from internal OPD database sources – namely the current police records management system (LRMS), including its adjunct field-based reporting module (FBR) and the communications computer-aided dispatch (CAD) system.

The purpose of the CrimeView product suite is to provide geospatial and temporal information about crime incidents, arrests, and calls for service. It uses minimal personal identifying information, and only in the two applications available to OPD

personnel, who are bound by the strict confidentiality rules previously detailed. The personal identifying information is sourced solely from internal OPD database sources and does not include information about an individual's immigration status. Oakland residents who may not have a legal immigration status have a right to privacy. The California Values Act (SB 54[4]) is enacted to ensure that (barring exceptions contained in the law) no state and local resources are used to assist federal immigration enforcement.

CentralSquare complies with all federal (FBI CJIS requirements), state (e.g., SB 54) and local laws (e.g., Oakland Sanctuary City Ordinance[5]) associated with use of collected law enforcement data. This includes, in the state of California and many individual jurisdictions, the prohibition on the use of facial recognition and the analysis of body worn camera video data.

E. Mitigations

OPD and CentralSquare use several strategies to mitigate against the potential for system abuse or data breaches.

System Mitigations

CentralSquare Technologies system provides security for customer data through a layered approach. CentralSquare uses CJIS-level security for storage and access as a best practice for managing customer operational data within. This security includes:

1. Access controls to the application.
2. Secure infrastructure hosted at the hosting facility.
3. Access limited to CentralSquare personnel with the required security approval. Analytics products, such as CrimeView and crimemapping.com, include data imported from the Customer's public safety systems (such as CAD and RMS).

The CentralSquare Cybersecurity Program Overview (see ***Attachment C***) "implements a series of comprehensive physical and logical controls that align with the NIST Cyber Security Framework and standards to provide a secure, layered defense for all hosted information. CentralSquare maintains annual Payment Card Industry (PCI) and Statement on Standards for Attestation Engagements (SSAE18) compliance through a series of ongoing assessments and security testing performed by a PCI Qualified Security Assessor and AICPA auditor. Adherence to these standards ensures all controls are met specific to access, transmission, processing, and storage of data."

The CentralSquare Cybersecurity Program overview also explains the framework for secure software development, vulnerability management, security incident response protocols, Government-standard cloud solutions (including audit compliance standards), and regulatory compliance protocols. The CentralSquare Analytics Product Security Overview (see ***Attachment D***) provides more security standards.

The City of Oakland-Central Square draft contract (see ***Attachment E; F for costing***) also

[4] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54

[5] https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=

provides language on the contractual security system commitments.

Safeguards in Alignment with Oakland and California Immigrant Legal Protections

CentralSquare's CrimeView product suite is geospatial by design. Minimal personally identifying information is only available in CrimeView Desktop and CrimeView Analytics. Use of these two applications is restricted to OPD personnel only, within a specific context. Users can only access these applications if they have a legitimate law-enforcement need for the information.

Data used in CentralSquare's CrimeView product suite originates solely from internal OPD database sources – namely the current police records management system (RMS), it's adjunct field-based reporting module (FBR), and the communications computer-aided dispatch (CAD) system.

Data Access Safeguards

Within the CrimeView Desktop and Analytics applications, OPD data cannot be accessed by anyone outside OPD. Additionally, OPD personnel using the CrimeView Analytics application must have a unique username and password, issued by the Crime Analysis Section manager.

Personnel Oversight

Department Genearl Order (DGO) **I 29: CRIME ANALYSIS SOFTWARE, explains that:** "While personally identifiable information (PII) is included in the data, the purpose of the product suite is to identify geographical and temporal trends and patterns. The data is not used to look at individuals as suspects or victims of crime."

This product suite does not contain a predictive component. It is used to assist experienced and trained crime analysts create informed analytical commentary supplemented by temporal and visual information. This information helps OPD commanders make sense of the tremendous amount of crime data generated in Oakland. Furthermore, CrimeView Desktop and CrimeView Analytics do not export external data – they only use OPD data that already exists in other systems.

Anonymization

Crimemapping.com is accessible by the public. Prior to any data being available via this application, it is anonymized to protect victim privacy and safety as well as the integrity of ongoing investigations.

F. Data Types and Sources

CentralSquare has created a file transfer protocol data feed to automatically acquire data into the CrimeView product suite. This data is currently limited to the police records management system (RMS), including the adjunct field-based reporting module (FBR) and communications CAD system.

The process by which CrimeView managages and purges expired data is as follows:

- An SQL script is run against the CAD and RMS databases.
- The output is written to a Parquet file and pushed to an S3 bucket in the AWS Government Cloud.
- The Parquet file is read, and the contained data is loaded to the CrimeView SQL database.
- The Parquet files may be kept for several months for troubleshooting purposes but are deleted at regular intervals to enforce data history trimming.
- The CrimeView SQL database is read, and an Elasticube database is rebuilt entirely using the data from SQL. No prior data is retained in the Elasticubes.
- Another synchronization script is run against the CAD and RMS databases to check primary keys and enforce the subscribed date range.

Any records in the CrimeView SQL database that are no longer in the source CAD and RMS database or are earlier than the subscribed date range are subsequently deleted from the CrimeView SQL database.

The following is an exhaustive list of datasets acquired by CentralSquare's CrimeView product suite from OPD data sources:

Data Source Collected	Collection Status	Database Location	Access Conditions
Arrests	Active	RMS	Only authorized OPD personnel
Field Contacts	Active	RMS	Only authorized OPD personnel
Incident Reports	Active	RMS	Only authorized OPD personnel
Calls for Service	Active	CAD	Only authorized OPD personnel
Stop Data	Active	FBR	Only authorized OPD personnel
Traffic Accident	Active	RMS	Only authorized OPD personnel

The purpose of the CrimeView product suite is to provide a geospatial view of crime in Oakland. This information assists police personnel, executives, and commanders with resource distribution, operational decisions, and long-term strategies.

G. Data Security

CentralSquare constantly processes large streams of criminal justice information (CJI) and must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy[6]. CentralSquare, along with its partner at Amazon Web Services (AWS) Government have developed strong CJIS-compliant data security protocols.

Supporting documentation from CentralSquare is attached: CentralSquare's

[6] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Cybersecurity Program Overview and CentralSquare's Analytics Product Security Overview.

a. Account Management – OPD personnel who use CrimeView Desktop must be seated crime analysts, with sole access to their computer and the ArcGIS desktop application with the Desktop extension. OPD personnel who use CrimeView Analytics must have a unique username and password to access the application. The users have access to accounts that are created, deleted, and managed by a local administrator within OPD (the Crime Analysis Section manager), who has special access permissions to the system.
b. Amazon Web Services (AWS) Government Cloud Protocols – CrimeView cloud data is stored in Amazon Web Services (AWS) Government and encrypted at rest using Microsoft BitLocker. CrimeView Cloud deployments hosted in AWS Government provide encryption through BitLocker (certified FIPS 140-2 encryption components and Microsoft BitLocker FIPS140-2-Jan2017-Certs-2932-2933- 2934).

c. CrimeView is hosted from an Amazon Web Services (AWS) Government facility. Each facility meets the stringent FBI CJIS Policy standards and guidelines with the following protection features on site:
    - Monitored by both fixed and pan-tilt/zoom security cameras
    - Protected by intrusion detection system
    - Two-factor authentication required for building access
    - Biometric iris authorization required for data center access
    - Extensive pre-employment background investigation process
    - On-site building security and data center monitoring staffed 24/7/365).

d. User Authentication and Authorization - All authorized users must maintain and enter a valid user ID and strong password combination to gain access to the system. Passwords must be changed every 90 days.

e. Personnel Screening, Training and Administration – CrimeView cloud access to implement and support the system is limited to personnel that have completed CentralSquare Technologies' CJIS compliant security approval process:
    - Access to the Cloud CrimeView infrastructure requires approved personnel to complete a layered secure login process that includes personally assigned passwords, advanced authentication to gain access to the CentralSquare Technologies network, and a secure access login to the applicable Cloud CrimeView domain, application, and SQL Server database.
    - Pre-employment background check.
    - Security-approved employees must successfully complete the CJIS On-Line Security and Awareness training and testing. Their certifications must be current and must be renewed every two years. In addition to CJIS required training, CentralSquare Technologies also does periodic training for security approved personnel on CentralSquare Technologies security policies.

- Criminal background checks have been completed on CentralSquare Technologies personnel as part of employee screening and by one or more law enforcement agencies (CentralSquare Technologies customers and, in some cases, state law enforcement agencies).
- CentralSquare personnel have been fingerprinted, and their prints have been submitted to one or more law enforcement agencies for a background check.
- Security approved personnel are the same personnel that are used for supporting customers with on-premises deployments of CAD, Mobile, RMS, and other CentralSquare products (including the CrimeView product suite.

H. Costs

A new proposed contract will cost the City $260,203.00 for the period of January 1, 2022 - December 21, 2026 (approximately $41,240 per year). The City of Oakland-Central Square draft contract (see ***Attachment D***) provides specific contract terms; ***Attachment E*** provides exact costing details.

I. Third Party Dependence

OPD relies on CrimeView's product suite as a private company to provide OPD with a robust geospatial application environment. The entire product suite, especially CrimeView Desktop, is unique and cannot be mirrored with any internal OPD system.

Section G above explains that Central Square utilizes Amazon Web Services (AWS) Government for cloud-support services, and that AWS Government has developed strong CJIS-compliant data security protocols. Additionally, Crimemapping.com is hosted in the Microsoft Azure non-government cloud, where only non-sensitive data is stored. Crimemapping.com records are first transmitted to the CrimeView AWS Government cloud then sent to the Crimemapping environment in Microsoft Azure. Hosted data at AWS and Azure is encrypted through Microsoft BitLocker and Microsoft FIPS 140-2 compliant encryption is utilized for data in transit (the same encryption components as CrimeView). Furthermore, CentralSquare also uses SecureLink Remote Access software (www.securelink.com) for remote access. SecureLink meets service level agreement (SLA) requirements and meets multiple regulatory requirements (such as FIPS and the FBI CJIS Security Policy), while maintaining customer network security.

J. Alternatives Considered

No other product or company can realistically provide OPD with advanced geospatial functionality, required by crime analysts who are creating detailed reports for OPD police personnel.

The CrimeView Desktop extension to ESRI's ArcGIS is unique. No other vendor provides this tool. The CrimeView Desktop application is crucial to the sustained operations of the Crime Analysis Section, allowing them to focus on analytical

observations and expanding the number of work products distributed to key OPD personnel.

K. Track Record of Other Entities

Many other police agencies in the U.S. use the CrimeView product suite (a complete list is not available from the vendor). OPD is aware that the following agencies utilize the software:

- San Diego Harbor Police. This agency runs an intelligence-led policing strategy using CrimeView Analytics;
- OPD staff has personal experience using the CrimeView product suite while employed by the City of Richmond, CA, as the individual analyst. Having this powerful geospatial application meant that one analyst could serve the entire agency with timely actionable geospatial and temporal information;
- Bedford Police Dept. (Texas);
- St. James Parish Sheriff's Office (Louisiana); and
- Arizona State University Police Dept. (Arizona)

Attachments

A. Omega Desktop Manual
B. CrimeView Analytics Overview
C. CentralSquare Cybersecurity Program Overview
D. CentralSquare Analytics Product Security Overview
E. City of Oakland-Central Square draft contract
F. Contract Pricing Document

DEPARTMENTAL GENERAL ORDER

I 29: CRIME ANALYSIS SOFTWARE

Effective Date:

Coordinator: Criminal Investigations Division, Crime Analysis Unit

---

CRIME ANALYSIS SOFTWARE

The purpose of this order is to establish Departmental policy and procedures for the use of Crime Analysis Software.

A. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the Oakland Police Department's (OPD) use of crime analysis software. The OPD Crime Analysis Section, part of the Criminal Investigations Division (CID) uses crime analysis software to examine crime patterns and provide OPD personnel with timely and useful information to assist in reducing crime in the city.

B. Purpose of the Technology: *The specific purpose(s) that the surveillance technology is intended to advance*

OPD uses information from the Crime Analysis Section to make data-informed decisions on how to deploy its limited resources toward reducing crime and completing investigations. Crime that occurs each year in Oakland can be analyzed by dedicated crime analysts, who decipher trends and patterns. This analysis helps OPD Commanders to undertake proactive approaches to crime deterrence. Data-driven analysis is one of the hallmarks of modern policing. Crime data analysis helps OPD deploy limited personnel effectively and while avoiding random deployments that may negatively impact Oakland communities. Police departments need geographical analytic technology to illuminate crime trends and undercover actionable information for crime investigations.

C. Description of The Technology: *the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.*

Crime analysis software, such as CentralSquare's "CrimeView" product suite[1], comprises specialized applications for dedicated crime analysts. Analysts with these unique software applications can use the applications to integrate OPD's Computer-Assisted Dispatch (CAD) and Law Records Management System (LRMS) data into a geographical interface, such as ESRI's ArcGIS[2] (geographic information system) enterprise mapping software. These applications use only internal OPD databases, primarily the CAD and LRMS systems. They can be connected to other internal OPD databases, such as OPD's gunshot location detection system ("ShotSpotter") application[3].

Crime analysis software lets analysts look at types of crimes and crime locations from a holistic geographical perspective. Analysts can view all crimes of a certain type across the entire geography of the city. This lets geographical clustering and patterning emerge that wouldn't be immediately obvious without viewing them on a map. Queries in this application can be tailored to the entire city down to the beat level, depending on the crime type being analyzed. This type of software assists analysts in identifying trends, patterns, and areas high numbers of specific crimes. Coupled with temporal analysis, the analysts can produce meaningful reports that assist police commanders to make deployment and investigative decisions.

CentralSquare's CrimeView product suite comprises three applications:

- CrimeView Desktop is a specialized desktop application that runs as an extension to ESRI's ArcGIS mapping application. Data is hosted within the City of Oakland's Information Technology Department (ITD);
- CrimeView Analytics is a cloud-based software-as-a-service (SaaS) that is hosted in CentralSquare's CJIS[4]-compliant cloud. This application is available to OPD personnel;
- Crimemapping.com is a public-facing SaaS application that provides a map-based view of crime incidents in Oakland. This application complements the City's already existing ITD-based CrimeWatch open data initiative.

While personally identifiable information (PII) is included in the data, the purpose of the product suite is to identify geographical and temporal trends and patterns. The data is not used to look at individuals as suspects or victims of crime.

This product suite does not contain a predictive component. It is used to assist experienced and trained crime analysts create informed analytical commentary

[1] OPD relies on Central Square Crime View at the time of the production of this policy for its crime analysis software needs. OPD may choose a different crime analysis software vendor in the future as technology and OPD Crime Analysis Section needs evolve over time.

[2] https://www.esri.com/en-us/arcgis/about-arcgis/overview

[3] ShotSpotter recently purchased Forensic Logic which produces CopLink. OPD uses CopLink but no OPD data from CrimeView connects to CopLink via ShotSpotter; these are entirely separate systems. ShotSpotter data connected to CrimeView is a one-way integration; there is no migration from CrimeView to ShotSpotter and/or CopLink.

[4] CJIS = Criminal Justice Information Services Division: https://www.fbi.gov/services/cjis

supplemented by temporal and visual information. This information helps OPD commanders make sense of the tremendous amount of crime data generated in Oakland.

D. **Authorized Use**: *the specific uses that are authorized, and the rules and processes required prior to such use the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data*

The authorized uses of CentralSquare's CrimeView product suite are as follows:

CrimeView Desktop – This application is a license-based desktop application that is used only by trained and experienced crime analysts. The application is an extension to ESRI's ArcGIS enterprise mapping program. Each crime analyst has ArcGIS installed in his or her computer. The CrimeView Desktop extension is then installed by CentralSquare technicians. Only authorized users may have this application installed on their desktops; all OPD desktop machines require a unique username and password for access.

CrimeView Analytics – This application is an OPD-wide SaaS application. Only OPD sworn law enforcement personnel or authorized professional staff may access CrimeView Analytics. Users must be employees of OPD and passed all appropriate background checks and clearances. CrimeView Analytics users must access the system using a unique username and password. Access is granted and managed by CID management personnel.

OPD personnel authorized to use CrimeView Desktop and Analytics receive required security awareness training prior to using the system, which includes training to access data in CLETS[5], the FBI NCIC System[6] or NLETS[7]. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All CrimeView Desktop and Analytics users have received required training.

Users shall not use or let others use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to authorized investigations, internal audits, or for crime analysts to produce crime analysis reports.

[5] https://www.courts.ca.gov/4901.htm
[6] https://irp.fas.org/agency/doj/fbi/is/ncic.htm
[7] https://www.nlets.org/

E. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.*

CrimeView Desktop -- Authorized users include only (CID Commander) approved crime analysts.

CrimeView Analytics – Authorized users include all sworn personnel and OPD professional staff. Users requesting access must be vetted and approved by OPD CID management staff.

OPD data in the CrimeView product suite is owned by OPD and is drawn from OPD's underlying systems. OPD personnel using CrimeView Desktop or Analytics shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of CrimeView's product suite with OPD computers and mobile digital terminal (MDT) computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with CentralSquare. CrimeView Analytics users are managed through a centralized account management process by OPD CID management personnel.

F. ***Data Protection:*** *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms*

CentralSquare constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy. CentralSquare, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

CentralSquare maintains a security program for security managing access to its clients' data – particularly HIPAA and CJIS information. This includes a pre-employment background check, security training required by Federal CJIS regulations, and criminal background checks and fingerprints required by federal or state regulations.

G. ***Data Retention*** *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

CentralSquare's CrimeView product suite follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from the CentralSquare CrimeView product suite system.

H. **Public Access**: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Crimemapping.com is the current name of the public facing product of the crime analysis software; this public portal provides the public with a map-based view of crime incidents in the City of Oakland.

Information available to the public via the crimemapping.com application is limited to information that falls under the release of information outlined in the California Public Records act.

- Offense Type (assault, robbery, burglary, theft, and so on)
- Incident Number
- Agency
- Date and time

Location information is not currently displayed in crimemapping.com. This is to protect victim privacy and safety as well as ongoing investigation integrity.

Exempted information includes any personally identifying information, including exact address locations, which could compromise ongoing investigations as well as witness or victim safety. Map pins are neutralized to the nearest block address or intersection, so as to protect the privacy of the public in instances where crimes are listed near where people reside.

I. **Third Party Data Sharing**: *if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

No non-OPD personnel shall access CrimeView Desktop and Analytics. crimemapping.com is a public-facing application and may be accessed by any member of the public.

J. **Training:** *the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training*

All city, county, state, and federal agencies that use information from the CLETS must participate in the California Dept. of Justice's training programs to ensure all personnel are trained in the operation, policies, and regulations of each file that is accessed or updated. Training must include the requirement that CLETS information shall only be obtained in the course of official business. The person receiving this information must have a "right to know" and "need to know;" and trained in the possible sanctions and criminal and civil liabilities if the information is misused.

Training shall be provided only by the CA DOJ's training staff or another certified CLETS/NCIC trainer. At OPD, this four-hour in-person (or live virtual) training is administered by the Communications Division.

Specifically, the training includes the following:

- Initially (within six months of employment or assignment), OPD personnel must attend the four-hour in-person (or live virtual) training.
- Personnel must functionally test and affirm their proficiency with the equipment and operation (full accessor less than full access, depending on assignment) to ensure compliance with the CLETS and NCIC policies and regulations.

This is accomplished by completing the required training and the appropriate CLETS and NCIC Telecommunications Proficiency Examination published by the California Dept. of ~~Justcie~~Justice.

Biennially, OPD personnel must retest and reaffirm their proficiency to ensure compliance with the CLETS and NCIC policies and regulations. This is accomplished by the completion of the appropriate CLETS and NCIC Telecommunications Proficiency Examination published by the CA DOJ.

K. **Auditing and Oversight:** *the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.*

CrimeView Desktop is a single-use licensed desktop application. Auditing and oversight is conducted in--person by CID management personnel. The extension is installed on the Desktop version of ESRI's ArcGIS application. The only individuals that are authorized to use this program are crime analysts working at OPD in the Bureau of Investigations. The installation and use of the extension is overseen by the manager of the Crime Analysis Section. No other individual at OPD is authorized its use. The City's ESRI ArcGIS licensing and maintenance is overseen by the City's GIS section of IDT.

CrimeView Analytics access and use is managed by CID management personnel. Unsuccessful log-on attempts are logged. Inactive users are locked out and cannot be reinstated until they've been re-admitted by the system administrator (an OPD CID management staff member).

L. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

CentralSquare shall be responsible for all SaaS system maintenance per the OPD-CentralSquare contract. OPD and City IDT shall be responsible for all City and OPD-side hardware and software.

By Order of

LeRonne L. Armstrong

Chief of Police Date Signed:

CENTRALSQUARE

Attachment B
Four-minute read

CrimeView Analytics

Better Insight, Smarter Policing

WHAT IS THE PROBLEM

Law enforcement practices are under more scrutiny than ever before. Agencies need information and data that helps them deploy smart policing based on informed, data-driven decisions. There is a lot of data out there. But a lot of data doesn't necessarily translate into better decisions and protocols, and in fact can just be added noise that can lead to wasted time and effort.

WHAT ARE THE BENEFITS

CrimeView Analytics combines disparate data sources for easy analysis that empowers your agency to operate efficiently and effectively. With timely insight into trends, patterns and behavior, agencies can proactively respond to situations that promote officer and citizen safety. Utilizing Esri mapping technologies, CrimeView Analytics allows users to create powerful and easy-to-understand dashboards and reports to share with others. Delivered as a single solution from the AWS GovCloud, CrimeView Analytics provides agencies with configurable, easily accessible and visually relevant displays of measurable and achievable goals.

WHAT IS THE SOLUTION

Make your data work the way you need it to. Whether it is an alert to a situation that needs immediate attention, or an evaluation over a time period for process improvements, you'll be better equipped with CrimeView Analytics.

FEATURES

- Analysis and Dashboard Modes
- Esri Maps with User Data (i.e. districts, beats, etc.)
- On-Demand Queries
- Scheduled Report Generation
- Threshold Alerting
- Address Geo-verification
- Density Maps
- User Based Security

SMARTER PATROL, SMARTER POLICING

Bring analytics and mapping into your patrol work with actionable information for your agency's proactive policing strategies. Integrate with your Mobile system and use the Esri-based maps and components drill down to specific geo data, like districts. Simplify administration time by automatically generating and delivering role-based reports and dashboards to supervisors and authorities. Create briefing books that can restrict viewable data based on role, organizational unit, geography or crime priority. Enable threshold alerting to receive automatic live alerts as irregular activates occurs.

SECURE, PERMISSION-BASED ACCESS

Deployed in AWS GovCloud, your data is protected with world class security encryption that is CJIS, ITAR, and FIPS compliant. CentralSquare's proven identity management ensures complete CJIS compliance and user management, which Administrators can easily configure for existing and new users.

BRING DIVERSE DATA SETS INTO A COMMON VIEW

CrimeView Analytics aggregates data from disparate systems and displays it as one seamless experience. In one view, see summaries and correlations from your calls for service, incidents, arrests, field interviews, and much more.

DATA SETS

- Incidents
- Warrants
- Record
- Field Interviews
- Citations
- Arrest
- Accident

ANALYSES

- **Intelligence Analysis** – use Analysis mode to link incidents and records based on geographical area, person(s), etc.
- **Criminal Investigative Analysis** – use Analysis mode to visually represent criminal incidents, trends and serial patterns to assist in criminal investigations.
- **Tactical Analysis** – use Dashboard mode to show where, when and what crimes occurred to predict resource requirements and track progress.
- **Strategic Analysis** – improve strategic planning and budget allocation with macro analysis to deploy resources effectively.
- **Administrative Analysis** – create and present dynamic dashboards to visually show incident data/trends for internal, city and state leaders.
- **Operational Analysis** – analyze your department's response times, call times, average units dispatched and other key operational metrics by location, call type, officer, etc.

WHO WE ARE

CentralSquare Technologies is an industry leader in public safety and public administration software, serving over 7,650 organizations from the largest metropolitan city to counties and towns of every size across North America.

CentralSquare's broad, unified and agile software suite serves 3 in 4 citizens across North America. Our technology platform provides solutions for public safety, including 911, computer aided dispatch and records management. For public administration agencies, CentralSquare provides software for finance, human capital management, payroll, utility billing, asset management and community development.

More information is available at www.centralsquare.com.

7,650

AGENCY CUSTOMERS

3 in 4

CITIZENS SERVED ACROSS NORTH AMERICA

2000+

EMPLOYEES FOCUSED ON SERVING THE PUBLIC SECTOR

CENTRALSQUARE TECHNOLOGIES

Cybersecurity Program Overview

The CentralSquare Cybersecurity Program implements a series of comprehensive physical and logical controls that align with the NIST Cyber Security Framework and standards to provide a secure, layered defense for all hosted information. CentralSquare maintains annual Payment Card Industry (PCI) and Statement on Standards for Attestation Engagements (SSAE18) compliance through a series of ongoing assessments and security testing performed by a PCI Qualified Security Assessor and AICPA auditor. Adherence to these standards ensures all controls are met specific to access, transmission, processing, and storage of data.

- **Secure Software Development**
- **Vulnerability Management**
- **Incident Response**
- **Business Continuity Management**
- **Government Cloud**
- **Regulatory Compliance**

Secure Software Development

CentralSquare implements secure coding best practices throughout the development lifecycle. Where supported, CentralSquare-developed applications undergo rigorous automated and manual testing and analysis. The lifecycle approach ensures that security is embedded into every application we develop.

Secure Software Lifecycle Management:

- **Requirements & Design**
  - Annual OWASP-based Developer training
  - Application Readiness Assessments to identify security gaps
- **Software Construction/Development**
  - Developer IDE Code Analysis
  - Real-time feedback on coding best practices & potential security flaws
- **Deployment & Maintenance**
  - Weekly Security "Scrum" with key stakeholders to address open security flaws
  - Monthly review with Product Directors to address application security strategy & timelines

Static Application Code Analysis

- **Service:** Third Party Independent Service
- **Methodology**
  - Binary code scan, executed during software construction stage of SDLC
  - Performed in a non-runtime environment; evaluates both web and non-web applications
  - Inspect compiled versions for flaws, malicious code, back doors etc.
  - Risk-based approach to remediation

Dynamic Web Application Scanning

- **Service:** Third Party Independent Service & Internal Scan Utility
- **Methodology**
  - Phase 1: Spider phase. Enumerate exposed functionality & attack surface
  - Phase 2: Attack & detect exploitable vulnerabilities as the application operates
  - Baseline derived from SANS Top 25 & OWASP Top 10 vulnerabilities
  - Risk-based approach to remediation

Advanced Application Security Assessments

- **Service:** Third Party Independent Service
- **Methodology**
  - Penetration testing of web-based applications, executed testing/validation stage of SDLC
  - Phase 1: Active & passive discovery including vulnerability scan
  - Phase 2: Manual, authenticated assessment to identify logic flaws, privilege escalation etc.
  - Remediation required for all confirmed findings. Timeline dependent on severity + overall risk

Vulnerability Management

Scanning and Remediation

The CentralSquare Scanning and Remediation Program is a critical component of secure software development & maintenance. Through a holistic approach to vulnerability management, CentralSquare identifies and correlates application, network and system issues to ensure effective, timely remediation and resolution.

External Perimeter Scanning

- Frequency: Weekly, or Ad Hoc upon request
- Methodology
  - Detect & classify network and system vulnerabilities for all owned/leased/hosted IP ranges
  - Remediation or Risk Acceptance required for all confirmed issues
  - Remediation timeline dependent on severity + overall risk to the Business Unit

Payment Card Industry Vulnerability Scanning & Penetration Testing

- Service: Third Party Independent Service
- Frequency: Quarterly (Vulnerability Scan) & Annual (Penetration Test)
- Methodology
  - Detect & exploit vulnerabilities as per PCI scanning requirements
  - Segmentation testing to ensure logical separation of Card Data Environment
  - Remediation required for external issues w/CVSS score of 4.0 or higher, to maintain PCI compliance
  - Remediation required for internal issues identified as High or Critical, to maintain PCI compliance

Advanced Network Security Assessments

- Service: Third Party Independent Service, performed by Depth Security
- Frequency: Annual
- Methodology
  - Phase 1: Information Gathering, define attack surface
  - Phase 2: Cross-reference open services with known vulnerabilities
  - Phase 3: Penetration test of network perimeter
  - Phase 4: Attempt to compromise target systems

Application & Scanning Vulnerability Remediation Process

- Confirmed Critical vulnerabilities are driven to a 30 day remediation timeline
- Confirmed High vulnerabilities are driven to a 60 day remediation timeline
- Vulnerabilities are driven to remediation or risk acceptance, per prescribed timelines
- Open vulnerabilities are reported weekly, with remediation plans updated bi-weekly

Incident Response

The Security Incident Response Policy establishes the steps needed to properly handle information security incidents, both suspected and actual, at CentralSquare. Incidents can include any event that could disrupt the confidentiality, integrity, or availability of CentralSquare systems and/or company and customer information. Procedures for detecting and responding to incidents are in place and employees are aware of the appropriate escalation steps.

DETECTION

Signs of a security incident may be obvious or subtle. Electronic security incidents may not immediately appear to affect sensitive systems or information, but could occur in a supporting system that directly or indirectly allows access to this information. Thus, any unusual activity or irregularity to configuration of systems or applications can signify a breach. CentralSquare has multiple tools in place to alert on an incident, including but not limited to: Security Information & Event Managers (SIEM), Syslog, Intrusion Prevention Systems (IPS), Web Filtering Services, Web Application Firewalls, and Advanced Threat Protect Engines.

RESPONSE

- Assess the nature of the incident. Invoke the CentralSquare Playbook for Managing a Data Breach, if necessary.
- Determine if CentralSquare staff or customers are affected by the incident. If customers are affected, an immediate plan will be developed to mitigate the problem and notify affected individuals. If customers are impacted the CentralSquare legal team will be notified.
- Determine potential signs of fraud. If fraud is suspected, the Human Resources and Legal departments will be notified.
- CentralSquare will notify impacted staff and customers within two business days (48 hours) of a confirmed incident.

REPORTING

In the event of a confirmed security incident, a detailed report is written that includes;

- Affected staff, customers, data, computing systems, and other property
- Response steps
- Root cause analysis

TESTING

The incident response plan will be tested annually via one of the following methods, unless already invoked during the current year for a suspected or actual incident:

- Table top exercise. Each employee will simulate their response based on the scenario given.
- Simulated incident. Notify appropriate management staff in advance and schedule a date to begin test. Establish protocols that will distinguish the test from a real security incident.

REVISION

The incident response plan will be refreshed on an as-needed basis, not to exceed 12 consecutive months.

- After a confirmed incident, a lessons learned analysis will be performed with relevant policy revisions.

- All plan revisions are reviewed and approved by management.

Business Continuity Management

The Business Continuity Management program (BCM Program) is a process designed to oversee the CentralSquare's ability to provide adequate business and technology recovery plans, capabilities to manage recovery of operations, identification of resiliency risks and rapid response during a disaster recovery crisis event.

All CentralSquare business functions develops, maintains and continually improves business continuity and disaster recovery plans. The purpose of these Plans are to:

- Protect life, information and assets of CentralSquare, respectively.
- Conform to applicable regulatory, insurance and ethical business practices.
- Support and be in agreement with the CentralSquare's tactical and strategic business plans.
- Minimize the impact of Disaster on our clients, employees and the business associates to whom services are provided.

CentralSquare has a comprehensive BCM Program in place including.

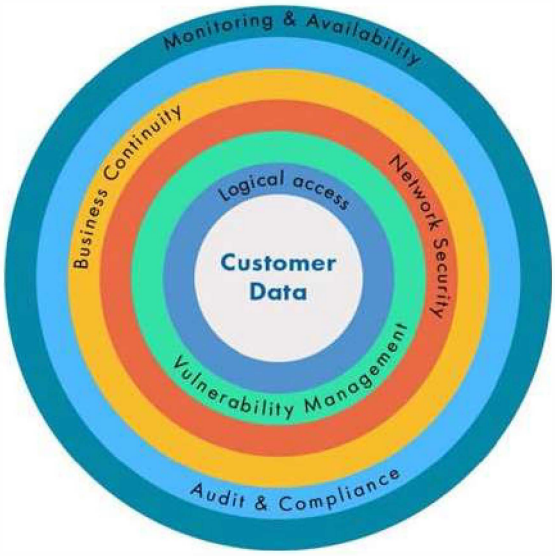
- Business Impact Analysis (BIA).
- Business Continuity Plan (BCP)
- Defined SLAs (Service Level Agreement), RTOs (Recovery Time Objective) and RPOs (Recovery Point Objective).
- Annual Disaster Recovery tests and/or Tabletop exercises, to include validation of recovered environment.
- Training and Annual Review

Government Cloud Solutions

The CentralSquare Cloud Security Program ensures 24x7 availability, integrity, and protection of customer information by leveraging a multi-faceted, layered approach to data security.

Physical & Environmental

Recorded Internal and External CCTV
Proximity Card Access Control to Facility; Dual Factor in Secure Areas
Intruder and Door Alarms
Best of Breed HVAC, Fire Suppression, and Physical Security



Monitoring & Availability

24x365 Staffed Operations Facility
24x365 Automated Network Monitoring, Incident Creation and Escalation
24x365 Distributed Denial of Service Mitigation
24x365 Intrusion Detection and Prevention Systems

Vulnerability Management

3rd Party and Internal Perimeter Vulnerability Scanning
Formal Application Security Scanning Program
Annual 3rd Party Penetration Testing
Centrally Managed Endpoint Protection on all Servers
Centrally Managed Patching and Operating System Hardening Program

Logical Access

VLAN Data Segregation
Extensive Deny-By-Default Access Control Lists
Multi-Factor Authentication for System Administration

Business Continuity

Daily Encrypted Backups stored offsite
Virtual Tape Backup Technology eliminates threat of lost physical media
Replication to Disaster Recovery Location
Internet Redundancy and High Availability using Multiple Carriers

Audit Compliance

Annual SSAE16/ISAE 3402 Data Center Audit
Annual SSAE16 Operations Audit
Annual Control Self-Assessment
Annual PCI-DSS Compliance Audit
Defined Information Security Program and Policy Framework

Network Security

SSL and IPSEC VPN with 256 Bit Encryption
Data-At-Rest Secured with 256 Bit AES Encryption where available
Web Application Firewall Protection
Multi-layer Infrastructure Security Model

Regulatory Compliance

As a provider of public administration and public safety software to government organizations, CentralSquare is subject to a comprehensive set of regulatory and customer audit obligations. These requirements drive the security and compliance framework that governs the CentralSquare business strategy and its employees, products, processes, and technology.

Maintaining customer data security requirements and industry regulatory compliance helps enable CentralSquare to be a market leader, as well as a trusted partner for the customers we serve. Most importantly, it helps to ensure the safety of sensitive citizen information.

PCI DSS: Payment Card Industry Data Security Standard. CentralSquare is a Level 1 provider of credit card processing which means we store, process, and transmit over 6 million one-time and/or recurring credit card transactions per year on behalf of the citizens we serve. Level 1 compliance carries the most stringent requirements as directed by the PCI DSS standard. These requirements are becoming increasingly complex and challenging every year, as bad actors discover new and easier ways to exploit systems that process, store, or transmit credit card data.

Compliance requirements include but are not limited to the following: annual onsite audit at the CentralSquare Center of Excellence in Lake Mary, recurring internal and external system vulnerability scanning, and application penetration testing. If your role in CentralSquare is to perform duties such as customer support, Cloud administration, application development, or professional services, it is imperative that you understand the proper operating requirements when supporting the CentralSquare Cloud and associated Credit Card Data Environment. The methods in which you access, support, and administer systems in the CentralSquare Cloud must adhere to the requirements set forth by the PCI Council and the CentralSquare Security & Compliance Program.

Maintaining PCI compliance not only means that CentralSquare is adhering to the requirements of the PCI Council, but most importantly it means that we are providing a safe and secure operating environment for the citizens we serve every day.

SSAE18: Standards of Statements on Attestation Engagements, #18. The SSAE18 Audit Standard is governed by the American Institute of Certified Public Accountants [AICPA], and focuses specifically on Data Center Controls relevant to the Hosting of Customer Financial Records. These controls consist of people, processes, and technology implemented to protect customer financial data. Examples include change management for customer production systems and financial applications, physical and environmental data center systems, backup and disaster recovery planning, and proper authentication and authorization into hosted customer environments.

CentralSquare Cloud stores, processes, transmits, and hosts customer financial information and is therefore audited on an annual basis, per the SSAE18 Standard. The audit outcome, along with a formal Auditor Opinion, is detailed in the System and Organizational Controls Report, or SOC Report.

Customers often require the CentralSquare SOC report as part of their annual internal financial audit. The SOC Report is considered sensitive in nature, and should only be provided to active CentralSquare Cloud customers. A redacted version of the report is available for premise customers that process credit card data through the CentralSquare Cloud Hub environment, and a high-level attestation letter can be provided for prospective customers or for purposes of Request For Proposal (RFP).

Ensuring proper protections exist in CentralSquare hosted data centers proactively helps to enable a secure operating environment and successful overall customer experience.

CJIS: Criminal Justice Information Services. Governed by the Federal Bureau of Investigation, the CJIS regulation pertains to proper access, handling, transmitting, processing and storing of Criminal Justice Information, or CJI. Criminal Justice Agencies must comply with all aspects of the CJIS policy, which also extends to non-Criminal Justice Agencies such as CentralSquare.

CentralSquare has an obligation to comply with CJIS specifically for the development, installation, and support of Public Safety solutions that we provide to Criminal Justice Agencies for the purpose of interfacing with FBI CJIS systems that may contain CJI. These applications include CAD, RMS, MCT, OSMCT, Freedom, StateConnect, and Message Switch.

CJIS requirements also extend to the Support system in use by CentralSquare when accessing public safety environments. Currently, Securelink is the approved CJIS Customer Support system due to enhanced features such as multi-factor authentication and FIPS (Federal Information Processing Standard) 140-2 compliance.

CJIS requirements also extend to CentralSquare personnel. To be cleared for support access to customer environments that may contain CJI, employees must complete annual training with a test component, get fingerprinted, and be willing to undergo a background check should the customer require one.

CentralSquare is subject to CJIS audit at both the state and federal levels, as part of overall compliance for our public safety customers. Ultimately, the customer is responsible for ensuring vendor compliance with CJIS, which means the customer can engage CentralSquare for compliance assurances during any CJIS audit engagement.

HIPAA: Health Insurance Portability & Accountability Act. CentralSquare provides public safety software solutions to many customers that fall within the purview of HIPAA; therefore we must meet the Administrative, Technical, and Physical control specifications specific to the safeguarding of Protected Health Information, or PHI.

Specifically, CentralSquare is subject to the requirements of a Business Associate (BA) to a Covered Entity. A Covered Entity is defined as any provider (City, County, University, etc.) that processes, transmits, or stores Protected Health Information.

As a Business Associate, CentralSquare is bound by a Business Associate Agreement for each Covered Entity. Business Associate Agreements set forth requirements to ensure the protection and prevent the disclosure of health information, and set specific provisions for breach reporting as they relate to the exposure of PHI.

FERPA: Family Educational Rights and Privacy Act &
PPRA: Protection of Pupil Rights Amendment. FERPA and PPRA are Federal laws intended to protect the rights of students and their families, and the privacy of student education records. The law applies to all institutions that receive funds through the U.S. Department of Education.

CentralSquare is a solution provider to many educational institutions, and therefore must abide by the laws of FERPA & PPRA in regards to proper handling of student data.

GDPR: European General Data Protection Regulation. EU legislation took effect on May 25, 2018, GDPR is designed to protect the Personally Identifiable Information (PII) of European citizens. The scope of GDPR extends to citizens residing in EU member countries as well as citizens defined as residing in the European Economic Area.

Federal, State & Local Data Privacy, Handling, and Incident Reporting. The requirements for proper handling, security, and privacy of customer data can vary with each customer depending on federal, state, and /or local requirements. Certain states such as Florida impose laws such as the Florida Information Protection Act, or FIPA, requiring any entity that acquires, maintains, stores or uses personal information of individuals in the state to abide by specific requirements in regard to data breach reporting and records disposal. CentralSquare works closely with each customer to ensure that all data security requirements are addressed to satisfaction of the customer as well as state and local law.

Additional information regarding the CentralSquare Information Security Program can be obtained by contacting information.security@CentralSquare.com.

Analytics Product Security Overview

CentralSquare Technologies Analytics system provides security for Customer data through a layered approach. This security includes 1) Access controls to the application; 2) Secure infrastructure hosted at the hosting facility; 3) access limited to CentralSquare personnel with the required security approval. Analytics products, such as CrimeView and CrimeMapping, include data imported from the Customer's public safety systems (such as CAD and RMS).

CentralSquare Technologies Analytics products are deployed either on-premise at the Customer site or in a Cloud deployment. This document will primarily focus Cloud deployments. On-premise systems are protected by the customer through their physical and infrastructure security.

A common question regarding Analytics products is do these products store Criminal Justice Information (CJI) data. Analytics products does not directly query, display or store Criminal Justice Information (CJI) data. Analytics data imports exclude the import of CJI data. The imported data may include narrative fields referred to as "remarks." If the source data for remarks includes CJI data, CentralSquare recommends excluding remarks from the import process.

While the Analytics products do not import CJI, CentralSquare uses CJIS-level security for storage and access as a best practice for managing Customer operational data within Analytics.

<u>CrimeView Security (including Subsystems such as CrimeView Analytics, FireView Analytics, CrimeView Dashboard, FireView Dashboard, Advanced Reporting Module, and NEARme)</u>

1. Application security through CrimeView includes the following:
    - Role-based security restricts user access by agency, data sensitivity, and individual entities. The Customer's CrimeView system administrator controls user accounts and role-based security assignments.
    - CrimeView encryption of data in motion is through certified FIPS 140-2 encryption components. All data exchanged is encrypted CrimeView utilizes encryption components with the following FIPS 140-2 Certificates:
        - FIPS 140-2 Certificate 1337
        - FIPS 140-2 Certificate 1894

      Note: The encryption method is RSA, and the length is 2048 bit
    - The initial data load into CrimeView is extracted from the Customer's source system. This data is transmitted from the Customer's site utilizing an encrypted transfer tool. Once the initial data is loaded on the servers – either on-premise or in a Cloud deployment, a data update process is initiated between the Customer's source systems and the Analytics CrimeView servers.
    - CrimeView Cloud data is stored in Amazon Web Services (AWS) Government and encrypted at rest using Microsoft BitLocker.
    - CrimeView Cloud deployments hosted in AWS Government provide encryption through Bit-Locker (certified FIPS 140-2 encryption components – Microsoft BitLocker FIPS140-2-Jan2017-Certs-2932-2933-2934).

2. CrimeView is hosted from an Amazon Web Services (AWS) Government facility. Each of these facilities meet the stringent FBI CJIS Policy standards and guidelines with the following protection features on site:
   - Monitored by both fixed and pan-tilt/zoom security cameras
   - Protected by intrusion detection system
   - Two-factor authentication required for building access
   - Biometric iris authorization required for data center access
   - Extensive pre-employment background investigation process
   - On-site building security and data center monitoring staffed 24/7/365

   The Cloud system infrastructure is managed and controlled by CentralSquare. CentralSquare Technologies currently hosts the Cloud CrimeView system at Amazon Web Services (AWS) Government.
   - The AWS Government deployment is through AWS infrastructure as a service. AWS allocates infrastructure based upon a CentralSquare defined template and CentralSquare security authorized staff setup storage, OS, DBMS (SQL Server), applications and security.
   - CentralSquare manages application and security updates as well as Operating System, DBMS and application upgrades at both hosting sites.
   - Hosting facility personnel do not have access to the system and do not perform system setup or maintenance.

3. Cloud CrimeView access to implement and support the system is limited to personnel that have completed CentralSquare Technologies' CJIS compliant security approval process.
   - Access to the Cloud CrimeView infrastructure requires approved personnel to complete a layered secure login process that includes personally assigned passwords, advanced authentication to gain access to the CentralSquare Technologies network and secure access login to the applicable Cloud CrimeView domain, application and SQL Server database.
   - Pre-employment background check.
   - Training - Each of security approved employee successfully completed CJIS On-Line Security and Awareness training and testing. Their certifications are current and must be renewed every two years. In addition to CJIS required training, CentralSquare Technologies also does periodic training for security approved personnel on CentralSquare Technologies security policies.
   - Criminal background checks have been completed on each of these personnel by CentralSquare Technologies as part of employee screening and by one or more law enforcement agencies (CentralSquare Technologies Customers and in some cases, State law enforcement agencies).
   - Fingerprints – each of these personnel have been fingerprinted and their prints have been submitted to one or more law enforcement agencies for background check.
   - Security approved personnel are the same personnel that are utilized for supporting Customers with on premise deployments of CAD, Mobile, RMS and other CentralSquare products.

<u>CrimeMapping Security</u>

Crimemapping.com is hosted in the Microsoft Azure non-government cloud, where only non-sensitive data is stored. The Crimemapping architecture is like that of CrimeView, but Crimemapping data is presented to the public. Crimemapping.com records are first transmitted to the CrimeView AWS Government cloud then sent to the Crimemapping environment in Microsoft Azure. Hosted data at AWS and Azure is encrypted through Microsoft BitLocker and Microsoft FIPS 140-2 compliant encryption is utilized for data in transit (the same encryption components as CrimeView).

PROFESSIONAL SERVICES AGREEMENT

BETWEEN

THE CITY OF OAKLAND

AND CENTRALSQUARE TECHNOLOGIES

TABLE OF CONTENTS

EXHIBITS

Exhibit 1 **Statement of Work**
Exhibit 2 **End User License Agreement and Support Terms**
Exhibit 3 **Pricing and Payment Milestones**
Exhibit 4 **Security Provisions**
a. **CentralSquare Cybersecurity Program Overview**
b. CentralSquare Analytics Product Security Overview
Exhibit 6 **City Contract Compliance Provisions**
Exhibit 7 **City Schedules**

This Agreement to provide Professional Services and Related Products as applicable and as set for with specificity herein ["Agreement"] is by and between CentralSquare Tehnologies, a public safety software [INSERT NATURE OF ORGANIZATION AND WHERE ORGANIZED] located at 1000 Business Center Drive, Lake Mary, FL 32746 ("Contractor") and the City of Oakland ("City"), a municipal corporation, located at One Frank H. Ogawa Plaza, Oakland, California 94612, who agree as follows:

RECITALS

This Agreement is made with reference to the following facts and objectives:

A. **WHEREAS**, the City Council has authorized the City Administrator to enter into contracts for professional or specialized services if the mandates of Oakland City Charter Section 902(e) have been met; and

B. **WHEREAS**, Contractor is the developer of public safety software products and related professional services ["Services"]; and

C. **WHEREAS**, City is part of and provides information technology services to the various City departments, offices, and programs; and

D. **WHEREAS**, City wishes to acquire Contractor's Services and products as specifically set forth in this Agreement, including the Statement of Work ["SOW"] attached hereto.

E. **WHEREAS**, the following Exhibits and Schedules are attached to and incorporated by reference into this Agreement:

Exhibit 1 Statement of Work
Exhibit 2 Software Support Agreement
Exhibit 3 Pricing and Payment Milestones
Exhibit 4 CentralSquare Cybersecurity Program Overview
Exhibit 5 CentralSquare Analytics Product Security Overview
Exhibit 6 City Contract Compliance Provisions
Exhibit 7 City Schedules

NOW THEREFORE, THE PARTIES TO THIS Agreement COVENANT AND AGREE AS FOLLOWS:

1. Security

a. Contractor's Security Program

In entering into this Agreement, City is relying upon Contractor's averment that it maintains a Security program for managing access to City data – particularly HIPAA and CJIS information which includes 1) a Pre-employment background check, 2) security training required by Federal CJIS regulations, and 3) criminal background checks/fingerprints required by Federal or State regulations. Contractor's Security program is detailed in the Security Provisions Exhibit 4 Contractor's Cybersecurity Program Overview and Exhibit 5 Contractor's Analytics Product Security Overview. In addition, Contractor avers to provide City the required documentation (such as the CJIS Security Addendum Certification form and VPN documents).

b. System Security

(i) Contractor shall at all times maintain and ensure that all of City's information technology systems which Contractor interfaces with or has access to remain secure and do not through any of Contractor's actions or lack of action thereof including, but not limited to, ransomeware attacks upon Contractor, become vulnerable to breach, hacking into or in any way provide any unauthorized access to third parties. Contractor shall be liable for and indemnify City for all liabilities, claims, losses, damages and expenses, restorative or protective measures made necessary made necessary by any of the foregoing, including without limitation, reasonable attorney's fees.

(ii). Contractor shall not work on any City information technology system unless Contractor first contacts and obtains prior written authorization from the City's Director of Office of Information Technology, or his or her designee. Contractor warrants and represents that it will provide all information, reports, and data that fully informs the City with respect to any work, software deliverables, or products that the Contractor works on or which alter or affect the City's information technology systems, including without limitation, any source code and passwords necessary to access or make any such work, software, deliverables or products usable by the City.

c. Cloud Security

Contractor understands that, in contracting for Contractor's Cloud Storage Service is relying upon Contractor's representations that the methods and procedures it has in place to protect City's data as set forth in Exhibit X [INSERT CITE TO VENDOR'S SECURITY DOCUMENT], prevent unauthorized access to, corruption of and use of City's data including, but not limited to, ransomeware attacks upon Contractor. Contractor further warrants and represents that it shall be liable for and fully indemnify the City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from claims against City due to a breach

of or other unauthorized access to the systems Contractor uses to provide City the services hereunder.

d. **Data Incidents.** Contractor shall implement and maintain a program for managing unauthorized disclosure of, access to, or use of City Data however they may occur ("Data Incidents"). In case of a Data Incident, or if Contractor confirms or suspects a Data Incident, Contractor shall: (1) promptly, and in any case within 24 hours, notify City by email, telephone, in person, or by other real-time, in-person communication; (2) cooperate with City and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to City in notifying injured third parties; and (3) otherwise comply with applicable laws governing data breach notification and response. In addition, if the Data Incident results from Contractor's other breach of this Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Contractor shall (a) compensate City for any reasonable expense related to the Data Incident. Contractor shall give City prompt access to such records related to a Data Incident as City may reasonably request. City will treat such records as Contractor's Confidential Information pursuant to **Section b., below**. Contractor is not required to give City access to records that might compromise the security of Contractor's other customers.

In the event of a Data Incident, City will coordinate with Contractor on the content of any intended public statements or notices to the relevant authorities regarding the Data Incident.

This provision does not limit City's other rights or remedies, if any, resulting from a Data Incident.

2. Priority of Documents

In the event of conflicting provisions as between the following documents, except as otherwise expressly stated, the provisions shall govern in the following order: the Amendments to this Agreement, in reverse chronological order of adoption, this Agreement and its Exhibits. The Exhibits shall govern in numerical order as set out in this Agreement.

3. Conditions Precedent

a Contractor must provide City with the following before the Agreement will become effective:

(1). A copy of Contractor's City of Oakland Business Tax License which must be kept current for the duration of the Agreement and shall be attached to this Agreement as part of Exhibit 6

(2). A completed set of the City of Oakland Schedules which shall be attached to this Agreement as Exhibit 7;

b. Contractor and City must complete and agree upon and execute a Statement of Work before the Agreement will become effective and which shall be attached to this Agreement as Exhibit 1.

4. Statement of Work

Contactor avers and covenants to perform the services ("**Services**") and provide the deliverables ("**Deliverables**") specified in Exhibit 1**,** the Statement of Work including, but not limited to, the as requested or required Additional Items, Maintenance and Support for its Crimemapping.com and CrimeView Desktop products and providing its CrimeView Analytics product as a Software as a Service, all as set forth with specificity in the SOW

5. Term

This Agreement shall start when it is executed in full by the parties {"Effective Date"] and end on December 31, 2024. Should City decide, in its sole discretion, to exercise either or both of the authorized one-year extensions, and the parties mutually agree on the extensions, the Agreement may be extended until December 31, 2026.

6. City Requirements for Project Deliverables

Contractor avers and covenants to provide its Services and Deliverables which will include, but not be limited to, expanding the utility of Contractor's CrimeView Analytics and crimemapping.com products, licensing and providing maintenance and support for those products and providing CrimeView Desktop to City as a Software as a Service, all as set forth in the SOW.

7. Contractor Warranty and Indemnification of Services

a. Contractor will provide its software ["Software"] and Maintenance and Support Services under this Agreement "as is", without warranty, and will support that "Software" from the date of live operational use ("Go Live") in accordance with Contractor's End User License Agreement and Software Support terms attached hereto as Exhibit 2. Subscription services are also provided "as is", without warranty, and will be supported in accordance with the Contractor's subscription terms in Exhibit 2

b. Notwithstanding paragraph 7.a. above, Contractor warrants and represents that the Software does not contain any back door, time bomb, Trojan horse, worm, drop dead device, or other program or routine inserted and intended to provide a means of

unauthorized access to, or a means of disabling, or rendering the Software unusable or inoperable.

c. Contractor acknowledges that City is a provider of public and municipal services to the public and residents of the City of Oakland and that City's reliance on and use of Contractor's Deliverables will be vital to: (a) the business operations of the City; (b) the orderly and efficient provision of public and municipal services by the City; and (c) the health and safety of City's residents; and therefore, that any unauthorized interruption of City's business and operations could result in substantial liability to City. In recognition of City's status as a provider of such public and municipal services, Contractor warrants and represents that Contractor shall not at any time during the term of this Agreement and thereafter render the Software unusable or inoperable, or otherwise disable the Contractor's software, take possession of the Software or if any, the Hardware provided to City by Contractor or Contractor's subcontractors or in any way deliberately take actions limiting Contractor's liability under this Agreement. If Contractor takes any such actions, Contractor shall be liable for and indemnify City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from Contractor's actions.

d. The Services and Deliverables (a) will conform in all material respects to the Specifications

e. Contractor represents that it will use commercially reasonable efforts, including appropriate testing, to ensure that the Software does not contain viruses, contaminants, or other harmful code that may harm the Software, City systems or other City software.

f. Contractor represents that it owns or has the unencumbered right to license to City, the Deliverables and all results of Services delivered to City hereunder, including all required Intellectual Property Rights therein.

g. Contractor represents that it has the requisite experience, certifications, skills and qualifications necessary to perform the Services in: (i) a timely, competent, and professional manner, and (ii) accordance with applicable governmental requirements, statutes, regulations, rules and ordinances including, without limitation, applicable data privacy laws and regulations ("Law");

h. Contractor further warrants and represents that the methods and procedures it has in place to protect City's data as set forth in Exhibit 4 [Central Square Security Overview letter], prevent unauthorized access to, corruption of and use of City's data, Contractor further warrants and represents that, subject to the coverage limits of its Cyber Insurance, it shall be liable for and fully indemnify the City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from claims against City due to a breach of or unauthorized access to the systems Contractor uses to provide City the services hereunder.

i. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES MADE IN THIS AGREEMENT, THE CONTRACTOR MAKES NO REPRESENTATION, ACKNOWLEDGEMENT, CONDITION OR WARRANTY OF

ANY KIND WHATSOEVER UNDER THIS AGREEMENT OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY STATUTORY, EXPRESS, IMPLIED OR OTHER WARRANTIES OR ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE REGARDING ANY SERVICES, DELIVERABLE OR ANY OTHER PRODUCT DELIVERED TO THE CITY UNDER THIS AGREEMENT.

8. **Payments.`**

City shall pay Contractor the CrimeView Analytics, CrimeView Desktop and Crimemapping Services fees along with the annual Software License Fees and the Additional Items Reserve for those services City requests Contractor to provide, the not to exceed fees set forth in Exhibit 3 [Pricing and Payment Milestones].

9. [RESERVED]

10. Proprietary or Confidential Information

10.1 Confidentiality Obligations. Confidential Information shall mean all proprietary or confidential information disclosed or made available by the other Party pursuant to this Agreement that is identified as confidential or proprietary at the time of disclosure or is of a nature that should reasonably be considered to be confidential, and includes, but is not limited to, the terms and conditions of this Agreement, and all business, technical and other information (including without limitation, all product, services, financial, marketing, engineering, research and development information, product specifications, technical data, data sheets, software, inventions, processes, training manuals, know-how and any other information or material), disclosed from time to time by the disclosing Party to the receiving Party, directly or indirectly in any manner whatsoever (including without limitation, in writing, orally, electronically, or by inspection); provided, however, that Confidential Information shall not include the Content that is intended to be published on the website(s) of either Party.

10.2 Each Party agrees to keep confidential and not disclose to any third party and to use only for purposes of performing or as otherwise permitted under this Agreement, any Confidential Information. The receiving Party shall protect the Confidential Information using measures similar to those it takes to protect its own confidential and proprietary information of a similar nature but not less than reasonable measures. Each Party agrees not to disclose the Confidential Information to any of its Representatives except those who are required to have the Confidential Information in connection with this Agreement and then only if such Representative is either subject to a written confidentiality agreement or otherwise subject to fiduciary obligations of confidentiality that cover the confidential treatment of the Confidential Information.

10.3 Exceptions.

The obligations of this Section 10 shall not apply if the receiving Party can prove by

appropriate documentation, where appropriate, that such Confidential Information (i) was known to the receiving Party as shown by the receiving Party's files at the time of disclosure thereof, (ii) was already in the public domain at the time of the disclosure thereof, (iii) entered the public domain through no action of the receiving Party subsequent to the time of the disclosure thereof, (iv) is or was independently developed by the Contractor without access to or use of the Confidential Information; (v) was provided to the Contractor by a third party who, to the best of the Contractor's knowledge, was not bound by any confidentiality obligation related to such Confidential Information; or (vi) is required by law or government order to be disclosed by the receiving Party, provided that the receiving Party shall (i) notify the disclosing Party in writing of such required disclosure as soon as reasonably possible prior to such disclosure, (ii) use its commercially reasonable efforts at its expense to cause such disclosed Confidential Information to be treated by such governmental authority as trade secrets and as confidential.

10.4 Contractor acknowledges that City is subject to public disclosure laws and that City will comply with requests for information ("RFI"), as it is required to do under the federal Freedom of Information Act, California Public Records Act, City of Oakland Sunshine Act or judicial or administrative court order. Contractor acknowledges that an RFI may pertain to any and all documentation associated with City's use of Contractor's Services. Contractor further acknowledges that it is obligated to assist and cooperate with City by producing all documentation that City requests as responsive to the RFI so that City may comply with its statutory obligations. City agrees to give Contractor as timely written notice as possible of the RFI such that Contractor may oppose the RFI or exercise such other rights at law as Contractor believes it has. However, Contractor must produce to City all documents City requests as RFI responsive and City will comply with the RFI unless, within the time frame established by the statute, judicial or court order under which the RFI is made, Contractor procures a Temporary Restraining Order or similar injunctive relief from a court or other tribunal of competent jurisdiction ordering City not to comply with the RFI pending final determination of Contractor's protest of the RFI. Contractor further agrees to accept City's tender of defense and to defend City and pay all City costs of defense in any litigation brought against City with respect to City not complying with an RFI that Contractor protests and will hold City harmless against any claims, attorneys' fees, damages, fines, judgments, or administrative penalties, which may arise from any such actions.

11. Ownership of Results

Excluding the Contractor's intellectual property, or if applicable, any subcontractor intellectual property, any interest of Contractor or its Subcontractors, in specifications, studies, reports, memoranda, computation documents in drawings, plans, sheets prepared by Contractor or its Subcontractors under this Agreement shall be assigned and transmitted to the City. However, Contractor may retain and use copies for reference and as documentation of its experience and capabilities.

12. Amendments

Changes to this Agreement will only be made by mutually agreed upon Amendments in writing.

13. Limitation on Liability

(a) Either party's liability to the other party for any and all liabilities, claims or damages arising out of or relating to this Agreement [Direct Damages], howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability or otherwise, shall not, in the aggregate, exceed twice the total value of this Agreement as set forth in Exhibit 3 [Pricing and Payment Milestones].

(b) IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY PUNITIVE, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOST BUSINESS OPPORTUNITIES, LOSS OF USE OR EQUIPMENT DOWN TIME, AND LOSS OF OR CORRUPTION TO DATA) ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE LEGAL THEORY UNDER WHICH SUCH DAMAGES ARE SOUGHT, AND EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

(c) This limitation of liability shall not apply to Contractor's [Indemnification] obligations as set forth in this Agreement.

14. Reserved

15. Indemnification

(a) General Indemnification.

Notwithstanding any other provision of this Agreement, Contractor shall indemnify and hold harmless (and at City's request, defend) City, and each of their respective Councilmembers, officers, partners, agents, and employees (each of which persons and organizations are referred to collectively herein as "Indemnitees" or individually as "Indemnitee") from and against any and all liabilities (of every kind, nature and description), claims, lawsuits, losses, damages, demands, debts, liens, costs, judgments, obligations, administrative or regulatory fines or penalties, damages, (incidental or consequential) costs, actions or causes of action, and expenses, including reasonable attorneys' fees, (collectively referred to herein as "Actions") caused by or arising out of:

(i) A claim for personal injury (including death) or property damage to the extent based on the strict liability or caused by any negligent act, error or omission of Contractor;

(ii) Unauthorized use or disclosure by Contractor of Confidential Information as provided in Section 10 above.

(b) Proprietary Rights Indemnity. Contractor shall indemnify, defend, save and hold harmless Indemnitees from any and all actions arising out of third party claims that the Contractor's Services, or Software, if any infringes upon or violates the Intellectual Property Rights of a third party. If the Services or Software will become the subject of an Action or claim of infringement or violation of the Intellectual Property Rights of a third party, Contractor may, in addition to its obligation to defend and indemnify City hereunder, in its discretion, and at Contractor's sole expense: (1) procure for City the right to continue using the Services or Software; or (2) replace or modify the Services or Software so that no infringement or other violation of Intellectual Property Rights occurs, if City determines that: (A) such replaced or modified Services or Software will operate in all material respects in conformity with the then-current specifications for the Services or Software; and (B) City's use of the Services or Software is not impaired thereby. Contractor's obligations under this Agreement will continue uninterrupted with respect to the replaced or modified Services or Software as if it were the original Software. If Contractor concludes in its sole judgement that none of the foregoing options are commercially reasonable, and the City's use of the Contractor's Services or Software is permanently enjoined this Agreement and the license granted herein shall terminate.

(c) Contractor shall have no duty under Section 15 (b) and shall not be liable for any Actions arising from;

(1) modifications made to Contractor's Software or the Services by the City unless the City has made such modifications at the request or direction of Contractor;
(2) the Contractor having been required to conform to all or part of specific product designs of the City, provided that the Contractor has informed the City that any such requirement to conform may result in a claim under clause 16(b);
(3) the use by the City of Contractor's Software or Services or any part of them with programs, hardware, or software supplied by other parties, unless the Contractor has represented to the City that its Software or Services or any part of them are designated for use with such other programs, hardware, or software;
(4) use of Contractor's Software or Services or any part of them by the City in a manner contrary to the Contractor's specifications and/or documentation provided by or through the Contractor and accepted by the City;
(5) use of Contractor's Software or Services or any part of them by the City on any hardware for which the Software or Services or any part of them was not designed; or
(6) the City not using corrections to the Software or Services or any part of them made known and available by the Contractor.

(d) For the purposes of the indemnification obligations set forth herein, the term "Contractor" includes, without limitation, Contractor, its officers, directors, employees, representatives, agents, servants, sub consultants, and subcontractors.

(e) Contractor acknowledges and agrees that it has an immediate and independent obligation to indemnify and defend Indemnitees from any Action which potentially falls within this Indemnification provision, which obligation shall arise at the time an Action is tendered to Contractor by City and continues at all times thereafter, without regard to any alleged or actual contributory negligence of any Indemnitee. Notwithstanding anything to the contrary contained herein, if a claim, lawsuit or liability results from or is contributed to by the actions or omissions of an Indemnitee, Contractor's liability under this provision shall be reduced to the extent of such actions or omissions based upon the principle of comparative fault.

(f) City shall give Contractor prompt written notice of any Action and shall fully cooperate with Contractor in the defense and all related settlement negotiations to the extent that cooperation does not conflict with City's interests. Notwithstanding the foregoing, City shall have the right, if Contractor fails or refuses to defend City with Counsel acceptable to City, to engage its own counsel for the purposes of participating in the defense. In addition, City shall have the right to withhold payments due Contractor in the amount of reasonable defense costs actually incurred. In no event shall Contractor agree to the settlement of any claim described herein without the prior written consent of City.

(g) All of Contractor's Indemnification obligations hereunder are intended to apply to the fullest extent permitted by law (including, without limitation, California Civil Code Section 2782) and shall survive the expiration or sooner termination of this Agreement.

(h) Contractor's Indemnification obligations hereunder shall not be limited by the City's insurance requirements contained in Schedule Q hereof, or by any other provision of this Agreement.

16. Termination

(a) Termination for Breach. If Contractor breaches any material obligation under this Agreement and fails to cure the breach within 30 days of receipt of written notice from City of said breach, City may terminate the Agreement and, subject to the Limitation on Liability (Section 13), recover all Direct Damages it incurs as a result of Contractor's breach.

(b) Contractor may terminate this Agreement if City breaches a material provision of the Agreement and does not cure the breach within 30 days of written notice from Contractor of said breach. In such event, Contractor will be entitled to payment of all fees for Services or Deliverables the City has Accepted but not paid Contractor up to the date of termination.

(c) Bankruptcy. Either party may immediately terminate this Agreement if (i) the other party files a petition for bankruptcy or has filed against it an involuntary petition for bankruptcy which is not dismissed within 60 days of its filing, (ii) a court has appointed a receiver, trustee, liquidator or custodian of it or of all or a

substantial part of the other party's property, (iii) the other party becomes unable, or admits in writing its inability, to pay its debts generally as they mature, or (iv) the other party makes a general assignment for the benefit of its or any of its creditors.

(d) Termination for Convenience by City. City may terminate this Agreement for any reason at any time upon not less than sixty (60) days' prior written notice to Contractor. After the date of such termination notice, Contractor shall not perform any further services or incur any further costs claimed to be reimbursable under this Agreement, any Purchase Order, Change Order, or Change Notice without the express prior written approval of City. As of the date of termination, City shall pay Contractor for Services or Deliverables the City has Accepted but not paid Contractor

(e) Transition Services after termination. In connection with the expiration or other termination of this Agreement or the expiration of this Agreement, Contractor may provide transition services as requested by City. Contractor shall provide a quotation to City for any transition services, and shall not be obligated to provide any services until both parties have mutually agreed in writing to such quotation.

(f) Effect of Termination. Upon termination of this Agreement, City shall remove all Contractor Software from its computer system and certify in writing to Contractor that it has destroyed all Contractor Software and its associated documentation. Any City data in Contractor's possession shall either be returned to the City or destroyed as directed by the City.

17. Dispute Resolution

a. If dispute or disagreement among the Parties arises with respect to either Party's performance of its obligations hereunder, or any provision of or interpretation of the Agreement, the Parties agree in good faith to attempt to resolve such dispute or disagreement (a "Dispute") prior to submitting the Dispute to mediation, arbitration or litigation in accordance with this Section 17. Such resolution efforts shall involve the City Administrator of the City of Oakland and an executive officer of Contractor, together with such other persons as may be designated by either Party.

b. Any Party may commence said resolution efforts by giving notice, in writing, to any other Party. Such notice shall include at least a description of the Dispute and any remedial action that the Party commencing the resolution procedure asserts would resolve the Dispute. Upon receiving such notice, the Party against whom the Dispute is brought shall respond in writing within five (5) Business Days. The Parties shall then meet and confer in a good faith attempt to resolve the Dispute.

c If the Dispute has not been resolved within ten (10) Business Days after the Subsection 17.b. notice is given, said period to be extended by the parties' mutual agreement and, unless the Party initiating the Dispute does not wish to pursue its rights relating to such Dispute or desires to continue the Pre-Mediation Dispute Resolution, then such Dispute will be automatically submitted to mediation. The mediation will be conducted in Alameda County by a single mediator selected by the Parties to the Dispute by mutual agreement or by the use of the Commercial Arbitration Rules of the American Arbitration Association for selecting an Arbitrator ["AAA RULES"] The Parties to the Dispute shall evenly share the fees and costs of the mediator. The mediator shall have twenty (20) Business Days from the submission to mediation to attempt to resolve such Dispute. If the Dispute is not resolved within that time period, the parties will be entitled to pursue such matter by demanding arbitration under the AAA RULES or instituting litigation.

18. Implementation

A mutually agreed upon Project Schedule will be developed for implementation of the Project under this Agreement as defined in the Statement of Work. The Project Schedule will define timelines and responsibilities of each Party and may be modified at the mutual agreement of the Parties.

19. Bankruptcy

All rights and licenses granted to City pursuant to this Agreement are, and shall be deemed to be, for purposes of Section 365(n) of the U.S. Bankruptcy Code, licenses of rights to "intellectual property" as defined under Section 101 of the U.S. Bankruptcy Code. In a bankruptcy or insolvency proceeding involving Contractor, the parties agree that City, as licensee of such rights, shall retain and fully exercise all of its rights and elections under the U.S. Bankruptcy Code, and the provisions thereof shall apply notwithstanding conflict of law principles. The parties further agree that, in the event of the commencement of a bankruptcy or insolvency proceeding by or against Contractor under the U.S. Bankruptcy Code, City shall be entitled to a complete duplicate of any such intellectual property, including the source code for Contractor's Licensed Software which Contractor has placed in escrow as required under this Agreement and all embodiments of such intellectual property, to which City would otherwise be entitled under this Agreement, and the same, if not already in City's possession, shall be promptly delivered to City (a) upon any such commencement of a bankruptcy proceeding upon written request therefore by City, unless Contractor elects to continue to perform all of its obligations under this Agreement, or (b) if not delivered under (a) above, upon rejection of this Agreement by or on behalf of Contractor upon written request therefore by City. If, in a bankruptcy or insolvency proceeding involving Contractor, the provisions of the U.S. Bankruptcy Code referenced above are determined not to apply, City shall nevertheless be entitled to no less than the protection offered by the provisions of the U.S. Bankruptcy Code with respect to its entitlement to and rights to the use and possession of all intellectual property to which City has been granted rights under this Agreement notwithstanding the bankruptcy or insolvency of Contractor.

20. Assignment

Contractor shall not assign or otherwise transfer any rights, duties, obligations or interest in this Agreement or arising hereunder to any person, persons, entity or entities whatsoever without the prior written consent of **the City Attorney and City Administrator or their respective designees, which shall not be unreasonably withheld. City's consent to any assignment shall be conditioned upon retaining all rights it has at law against Contractor as Assigno**r. Any attempt to assign or transfer without such prior written consent shall be void. Consent to any single assignment or transfer shall not constitute consent to any further assignment or transfer. In the event that Contractor assigns this Agreement in compliance with this provision, this Agreement and all of its provisions shall inure to the benefit of and become binding upon the parties and the successors and permitted assigns of the respective parties.

21. Agents/Brokers

Contractor warrants that Contractor has not employed or retained any subcontractor, agent, company or person other than bona fide, full-time employees of Contractor working solely for Contractor, to solicit or secure this Agreement, and that Contractor has not paid or agreed to pay any subcontractor, agent, company or persons other than bona fide employees any fee, commission, percentage, gifts or any other consideration, contingent upon or resulting from the award of this Agreement. For breach or violation of this warranty, the City shall have the right to rescind this Agreement without liability or, in its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such fee, commission, percentage or gift.

22. Publicity

Any publicity generated by Contractor for the project funded pursuant to this Agreement, during the term of this Agreement or for one year thereafter, must be approved by the City in advance and will make reference to the contribution of the City of Oakland in making the project possible. The words "City of Oakland" will be explicitly stated in all pieces of publicity, including but not limited to flyers, press releases, posters, brochures, public service announcements, interviews and newspaper articles.

City staff will be available whenever possible at the request of Contractor to assist Contractor in generating publicity for the project funded pursuant to this Agreement. Contractor further agrees to cooperate with authorized City officials and staff in any City-generated publicity or promotional activities undertaken with respect to this project.

23. Conflict of Interest

(a) Contractor

The following protections against conflict of interest will be upheld:

(1) Contractor certifies that no member of, or delegate to the Congress of the United States shall be permitted to share or take part in this Agreement or in any benefit arising there from.

(2) Contractor certifies that no member, officer, or employee of the City or its designees or agents, and no other public official of the City who exercises any functions or responsibilities with respect to the programs or projects covered by this Agreement, shall have any interest, direct or indirect in this Agreement, or in its proceeds during his/her tenure or for one year thereafter.

(3) Contractor shall immediately notify the City of any real or possible conflict of interest between work performed for the City and for other clients served by Contractor.

(4) Contractor warrants and represents, to the best of its present knowledge, that no public official or employee of City who has been involved in the making of this Agreement, or who is a member of a City board or commission which has been involved in the making of this Agreement whether in an advisory or decision-making capacity, has or will receive a direct or indirect financial interest in this Agreement in violation of the rules contained in California Government Code Section 1090 et seq., pertaining to conflicts of interest in public contracting. Contractor shall exercise due diligence to ensure that no such official will receive such an interest.

(5) Contractor further warrants and represents, to the best of its present knowledge and excepting any written disclosures as to these matters already made by Contractor to City, that (1) no public official of City who has participated in decision-making concerning this Agreement or has used his or her official position to influence decisions regarding this Agreement, has an economic interest in Contractor or this Agreement, and (2) this Agreement will not have a direct or indirect financial effect on said official, the official's spouse or dependent children, or any of the official's economic interests. For purposes of this paragraph, an official is deemed to have an "economic interest" in any (a) for-profit business entity in which the official has a direct or indirect investment worth $2,000 or more, (b) any real property in which the official has a direct or indirect interest worth $2,000 or more, (c) any for-profit business entity in which the official is a director, officer, partner, trustee, employee or manager, or (d) any source of income or donors of gifts to the official (including nonprofit entities) if the income totaled more than $500 in the previous 12 months, or value of the gift totaled more than $350 the previous year. Contractor agrees to promptly disclose to City in writing any information it may receive concerning any such potential conflict of interest.

Contractor's attention is directed to the conflict of interest rules applicable to governmental decision-making contained in the Political Reform Act (California Government Code Section 87100 et seq.) and its implementing regulations (California Code of Regulations, Title 2, Section 18700 et seq.).

(6) Contractor understands that in some cases Contractor or persons associated with Contractor may be deemed a "City officer" or "public official" for purposes of the conflict of interest provisions of Government Code Section 1090 and/or the Political Reform Act. Contractor further understands that, as a public officer or official, Contractor or persons associated with Contractor may be disqualified from future City contracts to the extent that Contractor is involved in any aspect of the making of that future contract (including preparing plans and specifications or performing design work or feasibility studies for that contract) through its work under this Agreement.

(7) Contractor shall incorporate or cause to be incorporated into all subcontracts for work to be performed under this Agreement a provision governing conflict of interest in substantially the same form set forth herein.

(b) No Waiver

Nothing herein is intended to waive any applicable federal, state or local conflict of interest law or regulation.

(c) Remedies and Sanctions

In addition to the rights and remedies otherwise available to the City under this Agreement and under federal, state and local law, Contractor understands and agrees that, if the City reasonably determines that Contractor has failed to make a good faith effort to avoid an improper conflict of interest situation or is responsible for the conflict situation, the City may (1) suspend payments under this Agreement, or (2) terminate this Agreement, (3) require reimbursement by Contractor to the City of any amounts disbursed under this Agreement. In addition, the City may suspend payments or terminate this Agreement whether or not Contractor is responsible for the conflict of interest situation.

24. Validity of Contracts

The Oakland City Council must approve all Agreements greater than $15,000. This Agreement shall not be binding or of any force or effect until signed by the City Manager or his or her designee and approved as to form and legality by the City Attorney or his or her designee.

25. Governing Law

This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to its conflicts of laws principles. Any action or proceeding to enforce the terms of this Agreement shall be brought in the courts of Alameda County, Oakland, California and each party agrees to waive any objections to personal jurisdiction and venue in the courts of Alameda County, Oakland, California.

26. Headings

Headings and captions used to introduce Sections and paragraphs of this Agreement are for convenience, only, and have no legal significance.

27. Construction

(a) Acceptance or acquiescence in a prior course of dealing or a course of performance rendered under this Agreement or under any Change Order, or Change Notice, shall not be relevant in determining the meaning of this Agreement even though the accepting or acquiescing party has knowledge of the nature of the performance and opportunity for objection.

(b) The language in all parts of this Agreement and any Purchase Order, Change Order, or Change Notice, shall in all cases be construed in whole, according to its fair meaning, and not strictly for or against, either Contractor, City regardless of the drafter of such part.

28. Waiver

No covenant, term, or condition of this Agreement may be waived except by written consent of the party against whom the waiver is claimed and the waiver of any term, covenant or condition of this Agreement shall not be deemed a waiver of any subsequent breach of the same or any other term, covenant or condition of this Agreement.

29. Independent Contractor

(a) Rights and Responsibilities

It is expressly agreed that in the performance of the services necessary to carry out this Agreement, Contractor shall be, and is, an independent contractor, and is not an employee of the City. Contractor acknowledges and agrees that all of Contractor's employees and subcontractors are under the sole direction and control of Contractor and City shall have no authority over or responsibility for such employees and subcontractors of Contractor. Contractor has and shall retain the right to exercise sole direction and supervision of the services, and full control over the employment, direction, compensation and discharge of all persons

assisting Contractor in the performance of Contractor's services hereunder. Contractor shall be solely responsible for all matters relating to the payment of his/her employees, including compliance with social security, withholding and all other regulations governing such matters, and shall be solely responsible for Contractor's own acts and those of Contractor's subordinates and employees. Contractor will determine the method, details and means of performing the services described in **EXHIBIT 1.**

(b) Contractor's Qualifications

Contractor represents that Contractor has the qualifications and skills necessary to perform the services under this Agreement in a competent and professional manner without the advice or direction of the City. This means Contractor is able to fulfill the requirements of this Agreement. Failure to perform all of the services required under this Agreement will constitute a material breach of the Agreement and may be cause for termination of the Agreement. Contractor has complete and sole discretion for the manner in which the work under this Agreement is performed. Contractor shall complete and submit to City, Schedule M-Independent Contractor Questionnaire, prior to the execution of this Agreement.

(c) Payment of Income Taxes

Contractor is responsible for paying, when due, all income taxes, including estimated taxes, incurred as a result of the compensation paid by the City to Contractor for services under this Agreement. On request, Contractor will provide the City with proof of timely payment. Contractor agrees to indemnify the City for any claims, costs, losses, fees, penalties, interest or damages suffered by the City resulting from Contractor's failure to comply with this provision.

(d) Non-Exclusive Relationship

Contractor may perform services for, and contract with, as many additional clients, persons or companies as Contractor, in his or her sole discretion, sees fit.

(e) Tools, Materials and Equipment

Contractor will supply all tools, except those tools, materials, equipment specified herein, if any, required to perform the services under this Agreement.

(f) Cooperation of the City

The City agrees to comply with all reasonable requests of Contractor necessary to the performance of Contractor's duties under this Agreement.

(g) Extra Work

Contractor will do no extra work under this Agreement without first receiving prior written authorization from the City.

30. Attorneys' Fees

If either party commences an action or proceeding to determine or enforce its rights hereunder, the prevailing party shall be entitled to recover from the losing party all expenses reasonably incurred, including court costs, reasonable attorneys' fees and costs of suit as determined by the court.

31. Counterparts

This Agreement may be executed in any number of identical counterparts, any set of which signed by both parties shall be deemed to constitute a complete, executed original for all purposes.

32. Remedies Cumulative

The rights and remedies of either Party provided in this Agreement shall not be exclusive and are in addition to any other rights and remedies provided by law, including the California Uniform Commercial Code.

33. Severability/Partial Invalidity

If any term or provision of this Agreement, or the application of any term or provision of this Agreement to a particular situation, shall be finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then notwithstanding such determination, such term or provision shall remain in force and effect to the extent allowed by such ruling and all other terms and provisions of this Agreement or the application of this Agreement to other situation shall remain in full force and effect.

Notwithstanding the foregoing, if any material term or provision of this Agreement or the application of such material term or condition to a particular situation is finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then the Parties hereto agree to work in good faith and fully cooperate with each other to amend this Agreement to carry out its intent.

34. Access

Access to City's premises by Contractor shall be subject to the reasonable security and operational requirements of City. To the extent that Contractor's obligations under this Agreement or any Purchase Order, Change Order, or Change Notice, require the performance

of Services or Work by Contractor on City's property or property under City's control, Contractor agrees:

(i) to accept full responsibility for performing all Services or work in a safe manner so as not to jeopardize the safety of City's personnel, property, or members of the general public; and

(ii) to comply with and enforce all of City's applicable regulations, policies, and procedures including, without limitation, those with respect to security, access, safety and fire protection, City's policy against sexual harassment, and all applicable state and municipal safety regulations, building codes or ordinances.

35. Entire Agreement of the Parties

This Agreement supersedes any and all Agreements, either oral or written, between the parties with respect to the rendering of services by Contractor for the City and contains all of the representations, covenants and Agreements between the parties with respect to the rendering of those services. Each party to this Agreement acknowledges that no representations, inducements, promises or Agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party, which are not contained in this Agreement, and that no other Agreement, statement or promise not contained in this Agreement will be valid or binding.

36. Modification

Any modification of this Agreement will be effective only if it is in a writing signed by all parties to this Agreement.

37. Notices

If either party shall desire or be required to give notice to the other, such notice shall be given in writing, via facsimile and concurrently by prepaid U.S. certified or registered postage, addressed to recipient as follows:

(City of Oakland)
Oakland Police Department
Nicole Freeman
455 7th Street, 2nd Floor
Oakland, CA 94607

(Contractor)
CentralSquare Technologies
Attn: Legal/Contracts
1000 Business Center Drive
Lake Mary, FL 32746

Any party to this Agreement may change the name or address of representatives for purpose of this Notice paragraph by providing written notice to all other parties ten (10) business days before the change is effective.

38. No Third Party Beneficiary

This Agreement shall not be construed to be an agreement for the benefit of any third Party or parties, and no third party or parties shall have any claim or right of action under this Agreement

39. Survival

Sections (2, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 20, 25, 30 and 38) of this Agreement, along with any other provisions which by their terms survive, shall survive the expiration or termination of this Agreement.

40. Time is of the Essence

The Special Circumstances of this Agreement require each Party's timely performance of its obligations under this Agreement. Each Party agrees perform its applicable obligations for implementation in accordance with the mutually agreed upon Project Schedule.

41. Authority

Each individual executing this Agreement or any Purchase Order, Change Order or Change Notice, hereby represents and warrants that he or she has the full power and authority to execute this Agreement or such Purchase Order, Change Order or Change Notice, on behalf of the named party such individual purports to bind.

SO AGREED:

City of Oakland,
a municipal corporation

_____
(City Administrator's Office) (Date)

_____
(Department Head Signature) (Date)

Approved as to form and legality:

_____
(City Attorney's Office Signature) (Date)

CentralSquare Software Systems

_____
(Signature) (Date)

00200550
_____
Business Tax Certificate No.

_____
Resolution Number

ATTACHMENT A

Schedule Q
INSURANCE REQUIREMENTS
Professional/Cyber Liability Exposures
(Revised 1/13/2017:dkg)

a. General Liability, Automobile, Workers' Compensation and Professional Liability

Contractor shall procure, prior to commencement of service, and keep in force for the term of this contract, at Contractor's own cost and expense, the following policies of insurance or certificates or binders as necessary to represent that coverage as specified below is in place with companies doing business in California and acceptable to the City. sThe insurance shall at a minimum include:

i. **Commercial General Liability insurance** shall cover bodily injury, property damage and personal injury liability for premises operations, independent contractors, products-completed operations personal & advertising injury and contractual liability. Coverage shall be at least as broad as Insurance Services Office Commercial General Liability coverage (occurrence Form CG 00 01)

Limits of liability: Contractor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than $2,000,000 each occurrence. If such CGL insurance contains a general aggregate limit, either the general aggregate limit shall apply

separately to this project/location or the general aggregate limit shall be twice the required occurrence limit. Such limits may be met through a combination of primary and umbrella/excess coverages.

ii. **Automobile Liability Insurance.** Contractor shall maintain automobile liability insurance for bodily injury and property damage liability with a limit of not less than $1,000,000 each accident. Such insurance shall cover liability arising out of any auto (including owned, hired, and non-owned autos). Coverage shall be at least as broad as Insurance Services Office Form Number CA 0001.

iii. **Worker's Compensation insurance** as required by the laws of the State of California, with statutory limits, and statutory coverage may include Employers' Liability coverage, with limits not less than $1,000,000 each accident, $1,000,000 policy limit bodily injury by disease, and $1,000,000 each employee bodily injury by disease. The Contractor certifies that he/she is aware of the provisions of section 3700 of the California Labor Code, which requires every employer to provide Workers' Compensation coverage, or to undertake

self-insurance in accordance with the provisions of that Code. The Contractor shall comply with the provisions of section 3700 of the California Labor Code before commencing performance of the work under this Agreement and thereafter as required by that code.

iv. ***Technology Professional Liability*** *(Errors and Omissions) OR* ***Cyber Liability Insurance*** *appropriate to the Consultant's profession, with limits not less than* ***$2,000,000*** *per occurrence or claim,* ***$2,000,000*** *aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.*

b. Terms Conditions and Endorsements

The aforementioned insurance shall be endorsed and have all the following conditions:

i. Insured Status (Additional Insured): Contractor shall provide additional insured status including the City of Oakland, its Councilmembers, directors, officers, agents, employees and volunteers as insured's under the Commercial General Liability policy. General liability coverage can be provided in the form of an endorsement to the Consultant's insurance (at least as broad as ISO Form CG 20 10 11 85 or **both** CG 20 10, CG 20 26, CG 20 33, or CG 20 38; **and** CG 20 37 forms if later revisions used). A STATEMENT OF ADDITIONAL INSURED STATUS ON THE ACORD INSURANCE CERTIFICATE FORM IS INSUFFICIENT AND WILL BE REJECTED AS PROOF OF MEETING THIS REQUIREMENT; and

ii. Coverage afforded on behalf of the City, Councilmembers, directors, officers, agents, employees and volunteers shall be primary insurance. Any other insurance available to the City Councilmembers, directors, officers, agents, employees and volunteers under any other policies shall be excess insurance (over the insurance required by this Agreement); and

iii. Cancellation Notice: Each insurance policy required by this clause shall provide that coverage shall not be canceled, except with notice to the Entity; and

iv. Certificate holder is to be the same person and address as indicated in the "Notices" section of this Agreement; and

v. Insurer shall carry insurance from admitted companies with an A.M. Best Rating of A:VII, or better.

c. Insurance Interpretation

All endorsements, certificates, forms, coverage and limits of liability referred to herein shall have the meaning given such terms by the Insurance Services Office as of the date of this Agreement.

d. Proof of Insurance

Contractor will be required to provide proof of all insurance required for the work prior to execution of the contract. Failure to provide the insurance proof requested or failure to do so in a timely manner shall constitute ground for rescission of the contract award.

e. Subcontractors

Should the Contractor subcontract out the work required under this agreement, they shall include all subcontractors as insured's under its policies or shall maintain separate certificates and endorsements for each subcontractor. As an alternative, the Contractor may require all subcontractors to provide at their own expense evidence of all the required coverages listed in this Schedule. If this option is exercised, both the City of Oakland and the Contractor shall be named as additional insured under the subcontractor's General Liability policy. All coverages for subcontractors shall be subject to all the requirements stated herein. The City reserves the right to perform an insurance audit during the course of the project to verify compliance with requirements.

f. Waiver of Subrogation

Contractor waives all rights against the City of Oakland and its Councilmembers, officers, directors, employees and volunteers for recovery of damages to the extent these damages are covered by the forms of insurance coverage required above.

g. Evaluation of Adequacy of Coverage

The City of Oakland maintains the right to, acting reasonably, modify, delete, alter or change these requirements, with reasonable notice, upon not less than ninety (90) days prior written notice.

h. Higher Limits of Insurance

If the contractor maintains higher limits than the minimums shown above, the City shall be entitled to coverage for the higher limits maintained by the contractor.

k. Claims Made Policies

If any of the required policies provide coverage on a claims-made basis:
1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.
2. Insurance must be maintained and evidence of insurance must be provided ***for at least three (3) years after completion of the contract of work.***
3. If coverage is canceled or non-renewed, and not ***replaced with another claims-made policy form with a Retroactive Dat***e prior to the contract effective date, the Consultant must purchase "extended reporting" coverage for a minimum of ***three (3)*** years after completion of contract work.

END OF SCHEDULE Q – INSURANCE REQUIREMENT

			One-time Fees	**Recurring Renewal/Maintenance**			*Optional Year 1*	*Optional Year 2*
Application	**Software/Services**	**Qty**		5/1/2022-4/30/2023	5/1/2023-4/30/2024	5/1/2024-4/30/2025	5/1/2025-4/30/2026	5/1/2026-4/30/2027
IQ CrimeView Advanced Reports Annual Subscription Fee	Software	1		$ 9,975.00	$ -	$ -	$ -	$ -
IQ - CrimeView Dashboard Annual Subscription Fee	Software	1		$ 13,615.88	$ -	$ -	$ -	$ -
IQ CrimeView Desktop License Annual Maintenance Fee	Software	1		$ 5,622.75	$ 5,903.89	$ 6,199.08	$ 6,509.04	$ 6,834.49
Crimemapping.com	Software	1		$ -	$ -	$ -	$ -	$ -
Quote No. Q-63453								
Professional Services -- Complete P1 integration	Services	N/A	$ 11,700.00					
CrimeView Analytics: Designer/Admin License Subscription Annual Subscription Fee	Software	4		$ 3,000.00	$ 3,150.00	$ 3,307.50	$ 3,472.88	$ 3,646.52
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - RMS Arrests	Software	1		$ 2,952.84	$ 3,100.48	$ 3,255.51	$ 3,418.28	$ 3,589.20
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - Stop Data (Using field interview data template)	Software	1		$ 2,952.84	$ 3,100.48	$ 3,255.51	$ 3,418.28	$ 3,589.20

CrimeView Analytics: Single Data Set (Add'l Yr) Subscription Fee - 7 additional years data- RMS Arrests	Software	7		$ 3,500.00	$ 3,675.00	$ 3,858.75	$ 4,051.69	$ 4,254.27
CrimeView Analytics: Single Data Set (Add'l Yr) Subscription Fee - 7 additional years data - Stop Data	Software	7		$ 3,500.00	$ 3,675.00	$ 3,858.75	$ 4,051.69	$ 4,254.27
CrimeView Analytics: Standard (3 years data) Non-CST System Subscription - CAD Incident & RMS Incident	Software	1		$ 7,710.20	$ 8,095.71	$ 8,500.50	$ 8,925.52	$ 9,371.80
CrimeView Analytics: Standard (Add'l Year) System Subscription - 7 additional years data CAD Incidents & RMS Incidents	Software	7		$ 4,900.00	$ 5,145.00	$ 5,402.25	$ 5,672.36	$ 5,955.98
Quote No. Q-62250								
Professional Services	Services	N/A	$ 5,000.00					

The following Services and Software fees will only be invoiced upon authorization to proceed from the agency. The dates for the Software - Recurring Renewal/Maintenance period are estimated. The actual renewal period will begin on the Go-Live date of the software.

Quote No. Q-64054								
Professional Services -- CrimeView Analytics Upgrade	Services	N/A	$ 16,380.00					
CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - LPR	Software	1		$ 1,800.00	$ 1,890.00	$ 1,984.50	$ 2,083.73	$ 2,187.91

CrimeView Analytics: Single Data Set (3 years data) Non-CST Sys. Subscription - Shotspotter	Software	1		$ 1,800.00	$ 1,890.00	$ 1,984.50	$ 2,083.73	$ 2,187.91	
		Total	$ 33,080.00	$ 61,329.51	$ 39,625.56	$ 41,606.84	$ 43,687.18	$ 45,871.54	$ 265,200.6

The prices quantified above are for the software and services contained herein. If any additional software or services are requested, then a change order/amendment shall be entered into with requisite pricing. An increase in the CentralSquare Software licenses granted to the City will result in an increase in the Annual Renewal fees.

BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. 554-5184
Fax No. 554-5163
TDD/TTY No. 554-5227

M E M O R A N D U M

TO: Chief William Scott, Police Department
Tom Paulino, All City Departments via the Mayor's Office

FROM: Victor Young, Assistant Clerk

DATE: March 14, 2022

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed legislation:

File No. 220242

Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this Ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

If you have comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

cc: Lisa Ortiz, Police Department
Lili Gamero, Police Department
Diana Oliva-Aroche, Police Department
Sgt. Stacy Youngblood, Police Department
Andres Power, Mayor's Office

City and County of San Francisco
Master Report

City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102-4689

File Number: 220242 **File Type:** Ordinance **Status:** 30 Day Rule

Enacted: **Effective:**

Version: 1 **In Control:** Rules Committee

File Name: Administrative Code - Limits on Storage and Use of DNA Profiles **Date Introduced:** 03/08/2022

Requester: **Cost:** **Final Action:**

Comment:

Title: Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this Ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

Sponsors: Ronen; Walton

History of Legislative File 220242

Ver	Acting Body	Date	Action	Sent To	Due Date	Result
1	President	03/08/2022	ASSIGNED UNDER 30 DAY RULE	Rules Committee	04/07/2022	

[Administrative Code - Limits on Storage and Use of DNA Profiles]

Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this Ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. The Administrative Code is hereby amended by adding Chapter 96G, consisting of Sections 96G.1-96G.7, to read as follows:

CHAPTER 96G:

LIMITS ON POLICE DEPARTMENT USE AND STORAGE OF DNA PROFILES

SEC. 96G.1. DEFINITIONS.

For purposes of this Chapter 96G, the following terms have the following meanings.

(a) ***Terms related to DNA Profiles.***

"DNA Profile" means a digital representation of the pattern of an individual's DNA that may be stored in a DNA Database. DNA Profile does not include the physical tissue or other physical human material from which the DNA that is the subject of a DNA Profile is extracted and analyzed.

"Evidentiary DNA Profile" means a DNA Profile collected or analyzed as evidence or potential evidence of a crime, including but not limited to a DNA Profile derived from material in a rape kit following a sexual assault.

"Victim" means a person harmed as a result of a crime or alleged crime.

"Victim DNA Profile" means a DNA Profile known to belong to a Victim, including but not limited to a DNA Profile from a reference sample contributed by a Victim for purposes of comparison with Evidentiary DNA Profiles, and any Evidentiary DNA Profile determined to belong to a Victim.

(b) ***Terms related to DNA Databases.***

"DNA Database" means a database used to store DNA Profiles.

"CODIS Database" means a DNA Database that is subject to the rules and standards that apply to CODIS DNA Databases under state and federal law, including but not limited to FBI CODIS Quality Assurance Standards and federal and state CODIS accreditation standards. CODIS is an acronym that stands for Combined DNA Index Systems. CODIS Databases are maintained primarily to enable law enforcement to store and search DNA Profiles obtained from forensic evidence and attributable to putative perpetrators of crime. CODIS Databases include but are not limited to the

National DNA Index System, state DNA Databases such as the CAL-DNA Data Bank, and certain local DNA Databases operated by local law enforcement crime laboratories.

"Non-CODIS DNA Database" means a DNA Database that is accessed or maintained by the Police Department or other City departments and is not a CODIS Database. Non-Codis DNA Databases include but are not limited to any DNA Database used for elimination or decontamination purposes (sometimes referred to as a "quality control" or "quality assurance" database), and any DNA Database used for investigatory purposes that is not a CODIS Database.

SEC. 96G.2. PROHIBITIONS ON UPLOADING AND STORING CERTAIN DNA PROFILES.

(a) Except as required by state or federal law, neither the Police Department nor any other City department may upload or store a Victim DNA Profile in any Non-CODIS DNA Database. If a DNA Profile already stored in a Non-CODIS DNA Database is determined to be a Victim DNA Profile, the DNA Profile must be purged from that Non-CODIS DNA Database as soon as reasonably practicable following that determination.

(b) Except as required by state or federal law, neither the Police Department nor any other City department may store in any Non-CODIS DNA Database for longer than 60 days any Evidentiary DNA Profile. Any Evidentiary DNA Profile must be purged from any Non-CODIS DNA Database in which the Evidentiary DNA Profile has been stored for a period of 60 days.

SEC. 96G.3. DNA PROFILE PURGE REQUIREMENT.

By July 1, 2022, or 15 days after the effective date of the ordinance in Board File No. _____, establishing this Chapter 96G, the Police Department shall purge from all Non-CODIS DNA Databases all Evidentiary DNA Profiles that have been stored in a Non-CODIS DNA Database

for longer than 60 days, and all Victim DNA Profiles that have been stored in a Non-CODIS DNA Database for any length of time.

SEC. 96G.4. USE OF NON-CODIS DNA DATABASES ONLY FOR QUALITY ASSURANCE PURPOSES.

The Police Department and other City departments may access, search, or otherwise use any Non-CODIS DNA Database, including any Evidentiary DNA Profiles stored in the Non-CODIS DNA Database, only for the purpose of identifying and/or eliminating contamination in a sample from which DNA Profiles have been or may be identified, sometimes referred to as "quality assurance" or "quality control" purposes, and not for any law enforcement investigative purpose.

SEC. 96G.5. UNDERTAKING FOR THE GENERAL WELFARE.

In enacting this Chapter 96G, the City is assuming an undertaking only to promote the general welfare. It is not assuming, nor is it imposing on its officers and employees, an obligation for breach of which it is liable in money damages to any person who claims that such breach proximately caused injury.

SEC. 96G.6. NO CONFLICT WITH FEDERAL OR STATE LAW.

Nothing in this Chapter 96G shall be interpreted or applied so as to create any requirement, power, or duty in conflict with any federal or state law.

SEC. 96G.7. SEVERABILITY.

If any section, subsection, sentence, clause, phrase, or word of this Chapter 96G, or any application thereof to any person or circumstance, is held to be invalid or unconstitutional by a decision of a court of competent jurisdiction, such decision shall not affect the validity of the remaining

portions or applications of the Chapter. The Board of Supervisors hereby declares that it would have passed this Chapter and each and every section, subsection, sentence, clause, phrase, and word not declared invalid or unconstitutional without regard to whether any other portion of this Chapter or application thereof would be subsequently declared invalid or unconstitutional.

Section 2. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: */S/ Sarah Crowley*
SARAH CROWLEY
Deputy City Attorney

n:\legana\as2022\2200358\01587576.docx

FILE NO. 220242

LEGISLATIVE DIGEST

[Administrative Code - Limits on Storage and Use of DNA Profiles]

Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this Ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

Existing Law

There are no local laws that currently regulate the storage or use of DNA profiles stored in a quality assurance database, or other City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases").

Amendments to Current Law

This ordinance would prohibit the Police Department or other City deparment from uploading or storing a DNA profile known to belong to a crime victim ("Victim DNA Profile") in any Non-CODIS DNA database, and would require purging of any DNA profile uploaded to a Non-CODIS DNA Database and then subsequently determined to belong to a crime victim.

This ordinance would prohibit the Police Department or other City department from storing any DNA profile obtained from crime scene evidence, including but not limited to DNA profile obtained from a rape kit, (an "Evidentiary DNA Profile") in any Non-CODIS DNA Database for longer than 60 days, and would require purging of any such profile after 60 days.

This ordinance would require the Police Department to purge from all Non-CODIS DNA Databases all Evidentiary DNA Profiles stored for longer than 60 days, and all Victim DNA Profiles stored for any length of time, by July 1, 2022, or 15 days after the effective date of the ordinance.

This ordinance would limit the Police Department and other City departments to using any Non-CODIS DNA Database only for purposes of identifying and/or eliminating contamination of DNA samples, and not for any law enforcement investigative purpose.

Background Information

The CODIS is the Federal Bureau of Investigation (FBI) program to store and search DNA profiles obtained from forensic evidence and attributable to putative perpetrators. CODIS is comprised of the national database operated by the FBI, state databases (e.g., the CAL-DNA Data Bank), and local databases operated by local law enforcement crime laboratories. The use of CODIS DNA databases is strictly controlled under state and federal law, and crime laboratories must maintain accreditation as well as compliance with the FBI Quality Assurance Standards (QAS) to participate in CODIS. The state CODIS laboratory administers CODIS for the local crime laboratories and is responsible for ensuring statewide compliance with state and federal CODIS requirements.

The state CODIS laboratory and FBI do not administer or regulate non-CODIS databases used by local law enforcement.

The Police Department's crime lab, like many local crime labs, maintains a non-CODIS database of DNA profiles that the Police Department refers to as the "quality assurance" database or "QA Database." The Police Department Criminalistics Laboratory's Forensic Biology Unit Operating Procedures ("Procedures") explain that the Police Department's QA database has two components: "(a) A database of every single source and deduced evidence profile analyzed since tracking began in 2015, and (b) An elimination database of samples from lab staff members, lab visitors, workers required to enter the lab, and law enforcement elimination samples, for example, CSI team members."

The Procedures further state that "[t]he purpose of the QA Database is to identify potential contamination of evidence by staff, visitors, law enforcement personnel or other evidence samples and report it promptly to lab customers," but that "matches not due to contamination are also identified and communicated to investigators using this QA Database."

The California Department of Justice Division of Law Enforcement released a bulletin on March 1, 2022, to "to clarify some of the issues surrounding DNA databases and their current use by California's local law enforcement." The bulletin includes the following statement:

> Internal QC [or quality control] databases maintained by California's local law enforcement should only contain DNA profiles from plausible sources of potential contamination, such as laboratory staff and crime scene investigators. To the extent that QC databases contain DNA profiles derived from any other source, law enforcement personnel should ensure that the inclusion of those

> DNA profiles is reasonable and the individual remains an ongoing source of potential contamination.
> ….
> The California Department of Justice crime laboratories use internal QC databases that do not contain reference samples from victims. Additionally, the state CODIS database does not contain victim reference samples in any of the criminal indices.

n:\legana\as2022\2200358\01587593.docx

Print Form

Introduction Form

By a Member of the Board of Supervisors or Mayor

Time stamp
or meeting date

I hereby submit the following item for introduction (select only one):

- [x] 1. For reference to Committee. (An Ordinance, Resolution, Motion or Charter Amendment).
- [ ] 2. Request for next printed agenda Without Reference to Committee.
- [ ] 3. Request for hearing on a subject matter at Committee.
- [ ] 4. Request for letter beginning :"Supervisor _____ inquiries"
- [ ] 5. City Attorney Request.
- [ ] 6. Call File No. _____ from Committee.
- [ ] 7. Budget Analyst request (attached written motion).
- [ ] 8. Substitute Legislation File No. _____
- [ ] 9. Reactivate File No. _____
- [ ] 10. Topic submitted for Mayoral Appearance before the BOS on _____

Please check the appropriate boxes. The proposed legislation should be forwarded to the following:

- [ ] Small Business Commission
- [ ] Youth Commission
- [ ] Ethics Commission
- [ ] Planning Commission
- [ ] Building Inspection Commission

Note: For the Imperative Agenda (a resolution not on the printed agenda), use the Imperative Form.

Sponsor(s):

Ronen

Subject:

Administrative Code - Limits on Storage and Use of DNA Profiles

The text is listed:

Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

Signature of Sponsoring Supervisor: /s/Hillary Ronen

For Clerk's Use Only

From:	Saini, Nikita (BOS)
To:	BOS Legislation, (BOS)
Cc:	Somera, Alisa (BOS); Calvillo, Angela (BOS); Ronen, Hillary
Subject:	FW: Ordinance and digest for introduction - Limits on Storage and Use of DNA Profiles
Date:	Tuesday, March 8, 2022 2:39:42 PM
Attachments:	Ordinance_final for intro_3.8.22.DOCX Digest_final for intro_3.8.22.DOCX DNA leg Intro form.pdf

Hello all,

Supervisor Ronen intends on introducing an ordinance today which would prohibit SFPD from storing victim DNA profiles in their DNA database. I've attached the ordinance and digest from the City Attorney as well as the introduction form. The /s/ constitutes an electronic signature from Supervisor Ronen.

Please let me know if I need to provide any additional information/documentation.

Thank you.

Best,
Nikita

Nikita Saini
Legislative Aide
Office of Supervisor Hillary Ronen
925.286.2820/ nikita.saini@sfgov.org
https://sfbos.org/supervisor-ronen-district-9

From: Crowley, Sarah (CAT) <Sarah.Crowley@sfcityatty.org>
Sent: Tuesday, March 08, 2022 2:14 PM
To: Ronen, Hillary <hillary.ronen@sfgov.org>; Saini, Nikita (BOS) <nikita.saini@sfgov.org>
Cc: PEARSON, ANNE (CAT) <Anne.Pearson@sfcityatty.org>; ZAREFSKY, PAUL (CAT) <Paul.Zarefsky@sfcityatty.org>; BUTA, ODAYA (CAT) <Odaya.Buta@sfcityatty.org>; CHEESEBOROUGH, PAMELA (CAT) <Pamela.Cheeseborough@sfcityatty.org>
Subject: Ordinance and digest for introduction - Limits on Storage and Use of DNA Profiles

Privileged and Confidential Communication – Do Not Disclose

Supervisor Ronen and Nikita,

I'm attaching the following ordinance and related legislative digest for introduction:

> Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA

Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this ordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

For the clerk of the board, I am confirming that my electronic signature in the attached ordinance signifies that I approve this ordinance as to form.

Please let me know if you have any questions.

Thanks,
Sarah

Sarah A. Crowley
Deputy City Attorney
Office of City Attorney Dennis Herrera
(646) 498-5521 Cell

[Administrative Code - Limits on Storage and Use of DNA Profiles]

Ordinance amending the Administrative Code to prohibit the Police Department or other City departments from uploading or storing DNA profiles known to belong to crime victims ("Victim DNA Profiles") in any City DNA database that is not subject to the federal and state rules governing Combined DNA Index Systems ("CODIS") databases ("Non-CODIS DNA Databases"), and from storing DNA profiles obtained from crime scene evidence ("Evidentiary DNA Profiles") in any Non-CODIS DNA Database for longer than 60 days; to require that, by July 1, 2022, or 15 days after the effective date of this Oordinance, the Police Department purge from Non-CODIS DNA Databases Evidentiary DNA Profiles stored for longer than 60 days and Victim DNA Profiles stored for any length of time; and to limit the Police Department and other City departments to using Non-CODIS DNA Databases only for quality assurance purposes, and not for any investigative purposes.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in *~~strikethrough italics Times New Roman font~~*.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. The Administrative Code is hereby amended by adding Chapter 96G, consisting of Sections 96G.1-96G.7, to read as follows:

CHAPTER 96G:

LIMITS ON POLICE DEPARTMENT USE AND STORAGE OF DNA PROFILES

SEC. 96G.1. DEFINITIONS.

For purposes of this Chapter 96G, the following terms have the following meanings.

(a) ***Terms related to DNA Profiles.***

"DNA Profile" means a digital representation of the pattern of an individual's DNA that may be stored in a DNA Database. DNA Profile does not include the physical tissue or other physical human material from which the DNA that is the subject of a DNA Profile is extracted and analyzed.

"Evidentiary DNA Profile" means a DNA Profile collected or analyzed as evidence or potential evidence of a crime, including but not limited to a DNA Profile derived from material in a rape kit following a sexual assault.

"Victim" means a person harmed as a result of a crime or alleged crime.

"Victim DNA Profile" means a DNA Profile known to belong to a Victim, including but not limited to a DNA Profile from a reference sample contributed by a Victim for purposes of comparison with Evidentiary DNA Profiles, and any Evidentiary DNA Profile determined to belong to a Victim.

(b) ***Terms related to DNA Databases.***

"DNA Database" means a database used to store DNA Profiles.

"CODIS Database" means a DNA Database that is subject to the rules and standards that apply to CODIS DNA Databases under state and federal law, including but not limited to FBI CODIS Quality Assurance Standards and federal and state CODIS accreditation standards. CODIS is an acronym that stands for Combined DNA Index Systems. CODIS Databases are maintained primarily to enable law enforcement to store and search DNA Profiles obtained from forensic evidence and attributable to putative perpetrators of crime. CODIS Databases include but are not limited to the

National DNA Index System, state DNA Databases such as the CAL-DNA Data Bank, and certain local DNA Databases operated by local law enforcement crime laboratories.

"Non-CODIS DNA Database" means a DNA Database that is accessed or maintained by the Police Department or other City departments and is not a CODIS Database. Non-Codis DNA Databases include but are not limited to any DNA Database used for elimination or decontamination purposes (sometimes referred to as a "quality control" or "quality assurance" database), and any DNA Database used for investigatory purposes that is not a CODIS Database.

SEC. 96G.2. PROHIBITIONS ON UPLOADING AND STORING CERTAIN DNA PROFILES.

(a) Except as required by state or federal law, neither the Police Department nor any other City department may upload or store a Victim DNA Profile in any Non-CODIS DNA Database. If a DNA Profile already stored in a Non-CODIS DNA Database is determined to be a Victim DNA Profile, the DNA Profile must be purged from that Non-CODIS DNA Database as soon as reasonably practicable following that determination.

(b) Except as required by state or federal law, neither the Police Department nor any other City department may store in any Non-CODIS DNA Database for longer than 60 days any Evidentiary DNA Profile. Any Evidentiary DNA Profile must be purged from any Non-CODIS DNA Database in which the Evidentiary DNA Profile has been stored for a period of 60 days.

SEC. 96G.3. DNA PROFILE PURGE REQUIREMENT.

By July 1, 2022, or 15 days after the effective date of the ordinance in Board File No. _____, establishing this Chapter 96G, the Police Department shall purge from all Non-CODIS DNA Databases all Evidentiary DNA Profiles that have been stored in a Non-CODIS DNA Database

for longer than 60 days, and all Victim DNA Profiles that have been stored in a Non-CODIS DNA Database for any length of time.

SEC. 96G.4. USE OF NON-CODIS DNA DATABASES ONLY FOR QUALITY ASSURANCE PURPOSES.

The Police Department and other City departments may access, search, or otherwise use any Non-CODIS DNA Database, including any Evidentiary DNA Profiles stored in the Non-CODIS DNA Database, only for the purpose of identifying and/or eliminating contamination in a sample from which DNA Profiles have been or may be identified, sometimes referred to as "quality assurance" or "quality control" purposes, and not for any law enforcement investigative purpose.

SEC. 96G.5. UNDERTAKING FOR THE GENERAL WELFARE.

In enacting this Chapter 96G, the City is assuming an undertaking only to promote the general welfare. It is not assuming, nor is it imposing on its officers and employees, an obligation for breach of which it is liable in money damages to any person who claims that such breach proximately caused injury.

SEC. 96G.6. NO CONFLICT WITH FEDERAL OR STATE LAW.

Nothing in this Chapter 96G shall be interpreted or applied so as to create any requirement, power, or duty in conflict with any federal or state law.

SEC. 96G.7. SEVERABILITY.

If any section, subsection, sentence, clause, phrase, or word of this Chapter 96G, or any application thereof to any person or circumstance, is held to be invalid or unconstitutional by a decision of a court of competent jurisdiction, such decision shall not affect the validity of the remaining

portions or applications of the Chapter. The Board of Supervisors hereby declares that it would have passed this Chapter and each and every section, subsection, sentence, clause, phrase, and word not declared invalid or unconstitutional without regard to whether any other portion of this Chapter or application thereof would be subsequently declared invalid or unconstitutional.

Section 2. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: */S/ Sarah Crowley*
SARAH CROWLEY
Deputy City Attorney

n:\legana\as2022\2200358\01587576.docx

Skip to main content

Most Popular

1. Internet entrepreneurs far from the U.S. are inflaming political...
2. San Francisco LGBTQ activist Cleve Jones uprooted from Castro...
3. Only one U.S. county saw a larger share of people leave last year than...
4. This capt the

BAY AREA // SAN FRANCISCO

D.A. Chesa Boudin drops case against suspect allegedly linked to a property crime from rape exam DNA

Megan Cassidy

Updated: Feb. 15, 2022 7:30 p.m.

San Francisco District Attorney Chesa Boudin dropped charges against a woman allegedly linked to a property crime through DNA collected from her rape kit.
Gabrielle Lurie/The Chronicle

UPDATE: Woman linked to S.F. crime through rape-exam DNA speaks out: 'If I can't even trust the police, who can I trust?'

San Francisco District Attorney Chesa Boudin has dismissed the property crime case against a woman whose DNA collected from a rape kit was used to link her to a recent property crime, officials said Tuesday.

Officials said the case amounted to "fruit of the poisonous tree," meaning evidence that led to the arrest was gathered in a way that violated the defendant's rights.

Boudin declined to comment on the case, citing privacy concerns.

News of the dismissal comes a day after Boudin leveled a bombshell allegation that the San Francisco Police Department crime lab had used a rape victim's DNA evidence gathered years ago to tie her to an unrelated crime.

Police documents reviewed by The Chronicle appear to support this claim.

A 2016 report from the Police Department's Forensic Services Division laid out the evidence collected from a sexual assault examination, which included DNA gathered from an oral swab of the victim.

Another report, tied to a burglary incident in late 2021, states that "during a routine search of the SFPD Crime Lab Forensic Biology Unit internal quality database, a match was detected and verified." That match, the report states, came from DNA gathered from the same laboratory number that was listed in the 2016 sexual assault report.

It's standard practice to collect sexual assault victim's DNA to distinguish it from their perpetrators'. The victim's DNA profile may also be stored in a database to ensure that hasn't contaminated other DNA tests, Boudin said .

However, Boudin said, there was a "huge distinction" between collecting a victim's DNA as a control check and holding it indefinitely in a database used to identify criminals.

Boudin said on Monday it was unclear whether any other sexual assault victims have been arrested for later crimes based on evidence they submitted in a rape exam. His office believes that one of the police's DNA databases could include DNA profiles from rape victims collected over several years, and that this database is regularly used to search for matches to DNA found at crime scenes.

San Francisco Police Chief Bill Scott said that his office is still investigating the alleged practice and that he is committed to ending it should the claims prove true.

Boudin's announcement garnered national attention, with sexual assault victim advocates decrying the practice as yet another deterrent for a rape victim to come forward.

Camille Cooper, vice president of public policy at the Rape, Abuse & Incest National Network, called the practice a "horrifying and an egregious violation of the survivor's privacy."

"Survivors who undergo rape-kit exams have consented to the collection of their DNA for a very specific purpose: to catch the person who raped them," she said. "Storing a survivor's DNA in a database, or using it for any other purpose, is indefensible, and will discourage them from seeking medical care or reporting an assault."

San Francisco Supervisor Hillary Ronen and state Sen. Scott Wiener have both said they are weighing legislation at the city and state levels that would ban the

they are weighing legislation at the city and state levels that would ban the practice.

Megan Cassidy is a San Francisco Chronicle staff writer. Email: megan.cassidy@sfchronicle.com Twitter: @meganrcassidy

Written By
Megan Cassidy

Reach Megan on

Megan Cassidy is a crime reporter with The Chronicle, also covering cops, criminal justice issues and mayhem. Previously, Cassidy worked for the Arizona Republic covering Phoenix police, Sheriff Joe Arpaio and desert-area crime and mayhem. She is a two-time graduate of the University of Missouri, and has additionally worked at the Casper Star-Tribune, National Geographic and an online publication in Buenos Aires. Cassidy can be reached on twitter at @meganrcassidy, and will talk about true crime as long as you'll let her.

City of Oakland

Economic Development & Workforce Dept. Impact Report for Commercial Corridor Security Camera Grant Program

A. Description

Resolution No. 88717 C.M.S., as amended and adopted on June 24, 2021, appropriated $150,000 to fund cameras in business corridors in Council District 6 and Council District 7.

Funds will be granted to one or two Intermediary organizations (Intermediary) with ties to the impacted areas, who will purchase security cameras to be granted to businesses (Recipients) to place on their private property along the identified commercial corridors. Since a data-driven approach is the best way to ensure cameras are not deployed in a discriminatory, viewpoint-based, or biased manner, the City will rely on OPD data to identify areas with the highest number of service calls for criminal activity to deploy the security cameras (see Section **C. Location**, below).

The terms of the program, including the requirements outlined in this Impact Report and in the accompanying Use Policy, will be defined in the agreement between the City and the Intermediary. The Intermediary will manage the agreements with individual business Recipients who will be placing security cameras on their private property.

B. Purpose

The program responds to the requests of business owners and residents in the identified areas by implementing a systematic approach to strengthen business corridors in East Oakland through a comprehensive security camera program. The purpose of this program is to support the revitalization of historically underinvested commercial corridors by increasing safety for residents, shoppers, employees, and small business owners. This is consistent with the Crime Prevention Through Environmental Design (CPTED) framework which works by decreasing the ability to commit a crime and increasing the chances that the crime will be seen and reported by naturally integrating security measures into the community with the goal of increasing quality of life, decreasing the fear of crime and decreasing crime.[1]

The goals of the Security Camera Grant Program are twofold:

[1] https://www.oaklandca.gov/resources/crime-prevention-through-environmental-design-cpted

First, the presence of quality security cameras demonstrates to these majority-Black and Latinx small business communities in East Oakland the City's commitment to their safety and security and the City's investment in the community. This investment will enhance a culture of safety and security in the neighborhoods and along vital commercial corridors in East Oakland. There will be an immediate mitigating effect on illegal activity because security cameras will serve as a visual deterrent to potential criminal activity.

Second, installing security cameras assists in deterring crime and promotes overall crime prevention in commercial corridors. The Intermediary will register the security cameras with OPD's existing Register Your Security Camera program.[2] The cameras may capture video evidence that produces supporting information needed to build credible cases for prosecution. Over time, the video evidence may lead to a notable increase in prosecutions and convictions.

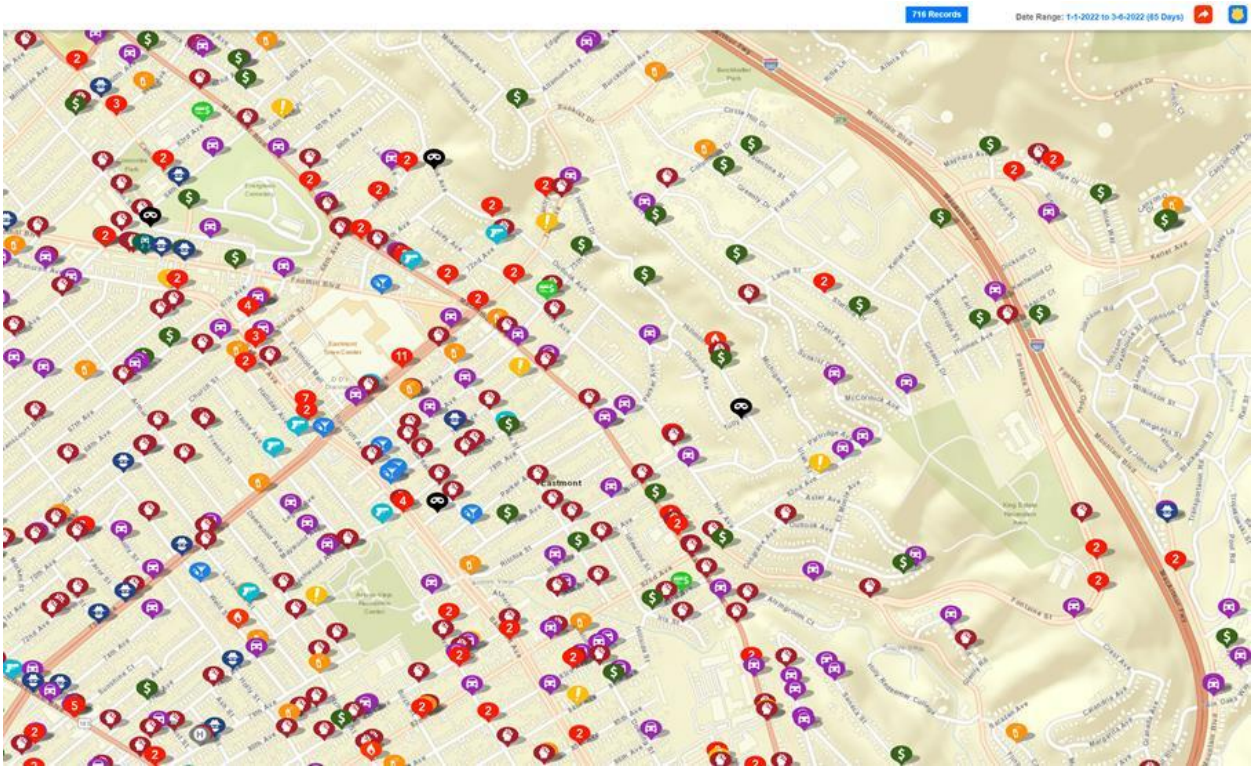
C. Location

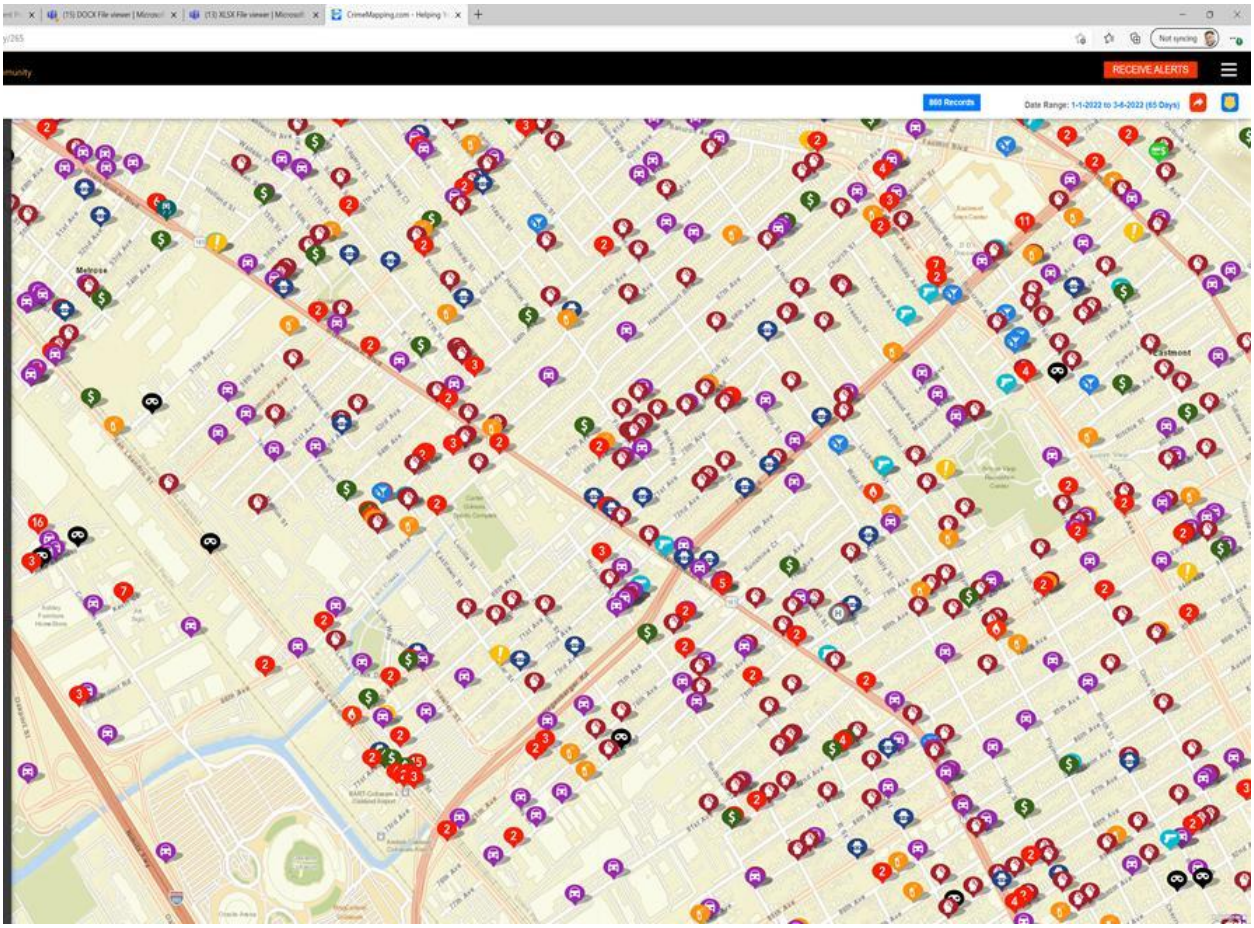
The grants will be issued to place cameras at strategic locations on private property on the premises of businesses in East Oakland. The identification of the priority areas for Program eligibility, including at least 3-4 areas in Districts 6 and 7, will be determined by crime levels and other public safety indicators, including areas where criminal activity has increased in the past several years during the COVID-19 pandemic. Preliminary analysis of available data shows that the following 4 Commercial Corridors in Council Districts 6 and 7 are likely to be a focus for the Program:

1. Eastmont Business Corridor (Foothill Ave/ MacArthur Blvd, 73rd-77th Ave)
2. Havenscourt Business Corridor (Bancroft, 64th – 67th Ave)
3. Hegenberger Rd (between Doolittle Dr and International Blvd)
4. Foothill Square

The following maps show the number of service calls related to the reported acts of criminal activity in those specified areas. These maps underscore the vital need for a security camera system in these areas. This data is derived from service calls to OPD over a recent 60-day period.

[2] https://www.oaklandca.gov/services/register-your-security-camera


716 Records
Date Range: 1-1-2022 to 3-6-2022 (65 Days)
Eastmont


RECEIVE ALERTS
860 Records
Date Range: 1-1-2022 to 3-6-2022 (65 Days)
Melrose
Eastmont

In October 2021, EWDD staff reviewed data by Police Beat (see **Attachment A**) and calculated the percentage change in crime reported between FY 2019-20 and FY 2020-21. While several Police Beats that include commercial corridors experienced double digit drops in reported crime, others saw increases. Of the 57 Police Beats across Oakland, 38 saw a reduction in crime reported. The 19 Police Beats that saw an increase in reported crime are concentrated in Central East Oakland and Deep East Oakland, including in the commercial districts identified above. Some of those commercial areas that saw double-digit increases in crime are shown in **Table 1**, below:

Table 1: Police Beat Change in Reported Crime FY 2019-20 and FY 2020-21

Police Beat	FY 2019-20	FY 2020-21	% Change
13Z-Montclair/Piedmont Pines/Central Hills	402	417	3.73%
16X-Lakeshore Ave./Trestle Glen/Crocker Highlands	167	175	4.79%
20X-Jingletown/part of Fruitvale District	811	871	7.40%
21Y-Upper Fruitvale	530	551	3.96%
27X-Fairfax	**482**	**532**	**10.37%**
27Y-Seminary	**551**	**711**	**29.04%**
30x–Havenscourt/ Arroyo Viejo	**735**	**865**	**17.69%**
34X-Elmhurst	**615**	**730**	**18.70%**

Focusing these resources along these identified corridors addresses longstanding racial disparities in access to City resources in neighborhoods with significant Black and Latinx and lower-income populations. For example, the 4 identified commercial corridors above are in census tracts with the following racial and income statistics, according to the OakDot Equity Toolbox:[3]

1. Eastmont - 97% People of Color (POC); 53% Low Income
2. Havenscourt - 92% POC; 45% Low Income
3. Hegenberger– 98% POC; 52% Low Income
4. Foothill Square - 88% POC; 40% Low Income

D. Impact

EWDD recognizes that all people have an inalienable right to privacy and are committed to protecting and safeguarding this right.

The proposed Security Camera Program does not seek to track movement of individuals. Nevertheless, EWDD recognizes that the public may be concerned that allocating City funds to place security cameras in public areas could capture information about individuals that could

[3] https://www.oaklandca.gov/resources/oakdot-geographic-equity-toolbox

potentially be used to track an individual's movement or be abused for other inappropriate purposes, including in the following specific areas:

- Identity capture. The public may be concerned that the cameras will capture personally identifiable information without notice or consent. Although the security cameras will be placed in private businesses where individuals do not have a reasonable expectation of privacy, and the data will only be made available to the City upon request for investigation of specific incidences involving suspected criminal activity or illegal dumping, camera footage may capture information about vehicle occupants, and/or license plate information that could be used to determine the registered owner. In addition, vehicle occupants or immediate surroundings (including addresses) may be pictured. As a result, it is possible that individuals with access to this data could do additional research to identify the individual.

- Misidentification. The public may be concerned that individuals may be misidentified as the person driving a vehicle and is committing a crime or engaging in illegal dumping. This could lead to government actions against such individuals in error.

- Activity monitoring. The public may be concerned that the cameras' data will enable individuals' behaviors to be revealed to and/or monitored by the City, their partners or affiliates, companies interested in targeted marketing, and/or the public. Such concerns may include basic information about when individuals are in certain locations, as well as concerns about what government or individuals may infer from this data (i.e., marital fidelity, religious observance, or political activity). Although video recordings and license plate numbers are gathered from public places, this could conflict with an individual's expectation of locational privacy.

E. Mitigations

To avoid the collection of large amounts of security footage by the City, these cameras will be purchased by the Intermediary who will grant the cameras to private business Recipients who will monitor the footage. Recipients will enter into agreements with the Intermediary, and the data collected by Recipients will not be considered public record. Footage will only be shared with OPD in the investigation of a crime or by OPW in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs.

The cameras will be purchased by the Intermediary and granted to Recipient Businesses to place on their business premises to monitor activity in areas in which the public does not have a reasonable expectation of privacy to reduce criminal activity. The cameras shall not be used for monitoring any residences. If the Camera is equipped with a "zooming" feature, such

feature shall be disabled and remain unused by Recipient. The Agreements between the Intermediary and the Recipients will outline the requirements contained in this report. No security camera purchased through this program will have any type of facial recognition technology imbedded within them

If the business vacates or moves from that location, Recipient shall inform the Intermediary of their intent to vacate or move from the location. The Intermediary reserves the right upon being informed of such intent to remove the security camera and equipment as necessary.

The data will be accessed only by the Recipient. No data will be stored with the City other than data requested by OPD in the investigation of a crime or by OPW in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs.

F. Data Types and Sources

1) Image, video recordings
2) License plate information as visible in video recordings
3) Annual Report*

*Since the intent of this program is to provide funds to the Intermediary to provide cameras for Recipient businesses, any auditing or reporting requirements will be addressed in the Annual Report submitted by the City to the PAC, per the requirements defined in the Use Policy.

G. Data Security

1) Data Collection
    i. The data from the cameras will not be collected or maintained by the City.
    ii. Signs will be placed in the locations where cameras are installed advising people that the area is under video surveillance.
2) Data Access
    i. Data will only made available upon request to OPD or OPW for the purposes of investigating reported crimes or illegal dumping, following the protocols of the existing City Camera Registry Program and OPW Illegal Dumping Surveillance Program.
    ii. The OPD Camera Registry Program allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation.

iii. Refer to OPW Illegal Dumping Surveillance Program guidelines for details on that program.

3) Data Protection
    i. Since the data will not be collected or maintained by the City, there should be no data protection concerns.
4) Data Retention
    i. Since the data will not be collected or maintained by the City, there should be no data retention concerns.
5) Public Access
    i. Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a security-related public records request, staff will consult with the City Attorney's Office for review and guidance.
6) Third-Party Data Sharing
    i. There is no third-party data sharing associated with this proposed Program.

H. Fiscal Cost

$150,000 was allocated in the FY 2021-2023 Biennial Budget to fund the Program. The fiscal costs for the Program include a grant to an Intermediary for the purchase of security cameras to be granted to and installed on the premises at Recipient businesses, plus any administrative costs to the Intermediary for administering the Program. Estimates obtained by EWD Staff for cost of the Security Camera itself have ranged from $150 for the basic security camera to $450 for the most sophisticated and versatile types of security equipment. The average cost of a security system and installation is $1,327, or between $617 and $2,039. A security service adds to installation complexities but provides 24-hour monitoring and other upgrades at a monthly fee. The cost of the monitoring has been estimated from $175 to $400 per month based upon the frequency and level of reporting desired.

I. Third Party Dependence:

There is no third-party dependence associated with the Program as proposed.

J. Alternatives:

Status Quo - Do not deploy the security camera program. The funds authorized by Council in the Biennial budget will not be spent to implement the program, and the program will not be realized. Criminal activity in the targeted commercial districts identified above could continue to increase, with no specific resources or economic development strategy to address public safety concerns in these commercial areas.

City Ownership and Installation of Security Cameras – Rather than work through an Intermediary, the City could purchase, own, and install the cameras on private property. This

approach would require the City to execute multiple grant agreements with individual small businesses, many of whom may be unable or unwilling to meet the City's contracting requirements, which could create a barrier to accessing the Program which may exacerbate rather than improve existing disparities. In addition, City control and monitoring of security camera footage would require significant City resources beyond the funds allocated for this program and City control and collection of data would raise additional privacy concerns requiring extensive mitigation measures.

K. Track Record:

As stated above, the City already has a Camera Registry Program that is a map-based database and a website. The Registry allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation. This Program would provide funding to commercial areas in East Oakland to close racial disparities in funding access to purchase costly security equipment so that more small businesses in majority Black and Latinx communities can participate in and realize the benefits of the existing City Camera Registry program. The City will continue to track and analyze crime and illegal dumping data along these commercial corridors pre- and post- camera to measure outcomes.

The City of Rancho Palos Verdes offers a similar Public Safety Reimbursement Program to allow neighborhoods and individuals to purchase public safety equipment such as security cameras. Rancho Palo Verdes provides a one-time reimbursement for half of the cost of a new public safety purchase, up to $2,000 for neighborhoods, and up to $100 for individuals and waives permit fees directly related to the installation of the approved purchase.[4] Philadelphia and Washington DC also offer similar programs.[5]

[4] https://www.rpvca.gov/1329/Public-Safety-Reimbursement-Program

[5] https://www.phila.gov/programs/business-security-camera-program/; https://ovsjg.dc.gov/service/private-security-camera-system-incentive-program

City of Oakland

Economic Development & Workforce Dept. Use Policy for

Commercial Corridor Security Camera Grant Program

April 7, 2022

A. Purpose

Resolution No. 88717 C.M.S., as amended and adopted on June 24, 2021, appropriated $150,000 to fund cameras in business corridors in Council District 6 and Council District 7.

Funds will be granted to one or two Intermediary organizations (Intermediary) with ties to the impacted areas, who will purchase security cameras to be granted to businesses (Recipients) to place on their private property along the identified commercial corridors. The City will rely on OPD data to identify areas with the highest number of service calls for criminal activity to deploy the security cameras.

The program responds to the requests of business owners and residents in the identified areas by implementing a systematic approach to strengthen business corridors in East Oakland communities through a comprehensive security camera program. The purpose of this program is to support the revitalization of historically underinvested commercial corridors by increasing safety for residents, shoppers, employees, and small business owners. The program goals are twofold:

First, the presence of quality security cameras demonstrates to our majority-Black and Latinx small business community in East Oakland the City's commitment to their safety and security and the City's investment in the community. Staff also believes there will be an immediate mitigating effect on illegal activity because security cameras will serve as a visual deterrent to potential criminal activity.

Second, installing security cameras not only assists in deterring crime but promotes overall crime prevention in our commercial corridors. Grant recipients will be strongly encouraged or required to register the security cameras with OPD's existing Register Your Security Camera program.[1] The cameras may capture video evidence that produces supporting information needed to build credible cases for prosecution. Over time, the video evidence may lead to a notable increase in prosecutions and convictions.

[1] https://www.oaklandca.gov/services/register-your-security-camera

B. Authorized Use

The cameras will be purchased by the Intermediary and granted to businesses Recipients to place on business premises (private property) along the identified commercial corridors to monitor activity in areas in which the public does not have a reasonable expectation of privacy to reduce criminal activity.

C. Data Collection

The data from the cameras will not be collected or maintained by the City. The only data that the City would have access to would be data collected upon request as evidence by OPD or OPW, which significantly limits the total amount of data available.

D. Data Access

Data will only made available upon request to OPD and OPW for the purposes of investigating reported crimes and/or illegal dumping, following the protocols of the existing OPD City Camera Registry Program and OPW Illegal Dumping Surveillance Program. The Camera Registry Program allows residents and business owners to register the locations of their video security systems with OPD. OPD will then be able to see where cameras are located. If a Recipient registers a camera, OPD will contact them if video footage is sought in connection to a criminal investigation.

E. Data Protection

Since the data will not be collected or maintained by the City, there should be no data protection concerns.

F. Data Retention

Since the data will not be collected or maintained by the City, there should be no data retention concerns.

G. Public Access

The only data that the City would have would be data collected upon request as evidence by OPD or OPW, which significantly limits the total amount of data available. Except where prohibited or limited by law, the public may access the City's video data through public records requests. However, prior to the release of any information to a surveillance-related public records request, staff will consult with the City Attorney's Office for review and guidance.

H. Third Party Data Sharing

There is no third-party data sharing associated with this proposed Program.

I. Training

The Intermediary and their staff who administer the Program will be trained on the City's Surveillance Technology Ordinance and Privacy Principals. The Intermediary will be bound, through the terms of their grant agreement with the City, to abide by the ordinance or face non-payment of funds under the contract.

J. Auditing and Oversight

The Economic and Workforce Development Department (EWDD) of the City will monitor performance of the Intermediary grantee to ensure compliance with the terms of the grant agreement. The Grant Agreement will include a requirement for a written Annual Surveillance Report concerning the grant funded Camera program. See **Attachment B** for a draft Grant Agreement between the City and the Intermediary.

The Intermediary organization will in turn manage the grants to individual business Recipients including compliance with the Program terms through a separate agreement between the Intermediary and each Recipient.

K. Maintenance

The security cameras and related equipment purchased with funds under this Program will be the property of the Recipient businesses. Any maintenance needs associated with the use of the security cameras or associated equipment will be the responsibility of the Recipient business.

ATTACHMENT B

OPD Crime Data by Police Beat

	FY19-20	FY20-21	% Change	FY21-22*
01X - Jack London Warehouse & Waterfront District	1,382	978	-29.23%	318
02X - Jack London Gateway to Mandela Pkwy	483	412	-14.70%	90
02Y - Prescott	473	358	-24.31%	57
03X - Chinatown to Lake Merritt Channel	938	564	-39.87%	138
03Y - Old Oakland to City Center	656	457	-30.34%	97
04X - Uptown & Lakeside	1,856	1,209	-34.86%	455
05X - Greater DeFremery	346	308	-10.98%	54
05Y - Port & former Oakland Army Base	211	162	-23.22%	30
06X - Durant Hoover	601	459	-23.63%	85
07X - McClymonds/Poplar/Clawson	658	657	-0.15%	113
08X - KONO to Harrison	1,938	1,335	-31.11%	396
09X - Piedmont Ave.	901	529	-41.29%	114
10X - Golden Gate	279	245	-12.19%	43
10Y - Longfellow & Santa Fe	314	274	-12.74%	58
11X - Idora Park & Fairview Park	340	235	-30.88%	47
12X - Temescal	1,094	428	-60.88%	151
12Y - Rockridge	988	383	-61.23%	130
13X - Upper Rockridge	165	165	0.00%	36
13Y - Hiller Highlands & North Hills	210	192	-8.57%	41
13Z - Montclair/Piedmont Pines/Central Hills	402	417	3.73%	95
14X - Adams Point	748	559	-25.27%	132
14Y - Upper Grand Ave.	663	429	-35.29%	122
15X - Peralta Heights & Haddon Hill	589	513	-12.90%	88
16X - Lakeshore Ave./Trestle Glen/Crocker Highlands	167	175	4.79%	25
16Y - Glenview	300	251	-16.33%	65
17X - Clinton Park	410	344	-16.10%	77
17Y - Bella Vista & Highland	398	395	-0.75%	76
18X - San Antonio Park	215	260	20.93%	61
18Y -	303	259	-14.52%	46
19X - EastLake/Embarcadero Cove/International Blvd. from Lake to 23rd Ave.	1,565	1,364	-12.84%	257
20X - Jingletown/part of Fruitvale	811	871	7.40%	159
21X - 23rd Ave./Central Reservoir	363	378	4.13%	61
21Y - Upper Fruitvale	530	551	3.96%	109
22X - Dimond/Oakmore/Lincoln Highlands	590	396	-32.88%	80
22Y - Woodminster/Redwood Heights/Cretmont/Bret Harte	529	549	3.78%	0
23X - part of Fruitvale	879	870	-1.02%	192
24X -	406	416	2.46%	78
24Y - Allendale	363	342	-5.79%	65

25X - Beulah Heights/Leona Heights/Laurel District	690	562	-18.55%	125
25Y - Merritt College/Skyline	165	116	-29.70%	27
26X - Melrose/Oakport/Coliseum Way	645	644	-0.16%	128
26Y - Lockwood	866	875	1.04%	170
27X - Fairfax	482	532	10.37%	85
27Y - Seminary	551	711	29.04%	160
28X - Maxwell Park	321	356	10.90%	54
29X - Picardy/Millsmont	667	643	-3.60%	129
30X - Havenscourt/Arroyo Viejo	735	865	17.69%	141
30Y - Eastmont/Eastmont Hills	643	619	-3.73%	118
31X - Coliseum/Airport/Airport Business Park	995	380	-61.81%	216
31Y - Brookfield Village/Columbian Gardens	927	731	-21.14%	175
31Z - Sobrante Park	283	316	11.66%	45
32X - Stonehurst/Durant Square	595	555	-6.72%	116
32Y - Los Palmas/Toler Heights	636	638	0.31%	151
33X - Woodland	721	799	10.82%	138
34X - Elmhurst	615	730	18.70%	125
35X - Kings Estate/Oak Knoll	597	627	5.03%	99
35Y - Sequoyah Heights/Elysian Fields/Chabot Park/Sheffield Village	286	306	6.99%	49

99X and 77X are used when an officer doesn't assign a beat

77X	1,169	738	-36.87%	176
99X	130	112	-13.85%	14

*partial year = July 1, 2021 to Sept. 15, 2021

GRANT AGREEMENT
BETWEEN THE CITY OF OAKLAND
AND [TBD Intermediary Organization]

This Grant Agreement (the "Agreement") dated July___, 2022 is made and entered into by and between the City of Oakland, a municipal corporation (the "City"), and the [TBD Intermediary Organization] ("Grantee").

RECITALS

A. The City wishes to enter into this Agreement with Grantee to provide funding to Grantee to purchase security cameras to be granted to recipient businesses ("Recipients") throughout designated commercial corridors in East Oakland. The data from the cameras will not collected or maintained by the City. The data collected by Recipients will not be considered public record. Footage will only be shared with the Oakland Police Department ("OPD") in the investigation of a crime or with the Oakland Public Works Department ("OPW") in the investigation of illegal dumping, pursuant to the guidelines of the existing Security Camera Registry and Illegal Dumping Surveillance programs. Signs will be placed in the camera locations advising people that the area is under video surveillance.

B. The City Council, pursuant to Resolution No. [TBD] C.M.S. has allocated grant funds to Grantee to fund its community-related programs and activities as specified herein.

Now therefore the parties to this Agreement agree as follows:

1. Grant

   Subject to the terms and conditions of this Agreement, the City agrees to provide a grant of funds to Grantee in an amount up to one hundred and fifty thousand dollars ($150,000.00) (the "Grant").

2. Scope of Work

   As a condition of this Grant, Grantee must diligently and in good faith perform the community-related work, services, and activities ("Work") specified in the **Scope of Work** attached to this Agreement as **Schedule A** and incorporated herein by reference.

   Grantee shall designate an individual who shall be responsible for communications with the City for the duration of this Agreement. The Project Manager for the City shall be **Juno Thomas.**

3. Agreement Documents and Provisions

   Grantee shall perform or arrange for the performance of Work under this Agreement in accordance with conditions of this Agreement including the attached Scope of Work in addition to City of Oakland rules, regulations and policies and applicable federal and state laws.

4. Time of Performance

The Grant term shall begin on [DATE/TBD] and shall end upon total grant disbursement and/or use, or upon either party's 30-day written notice.

5. Method of Payment

Grantee shall be paid for the performance of the Work set forth in the Scope of Work in accordance with the Program Budget included in the Scope of Work. Payments shall be made in the amounts stated in the Scope of Work and shall be based on actual eligible costs, fees and expenses incurred by Grantee for the Work. Payments shall be due upon completion of the Work or as otherwise specified in the Scope of Work. Grantee shall submit an invoice accompanied by an itemization of expenditures submitted for reimbursement prepared on the City's expense forms. Invoices shall state a description of the Work completed, itemized costs, fees and expense and the amount due.

The documents submitted shall be reviewed and approved for payment by the Project Manager. The City shall have sole and absolute discretion to determine the sufficiency of supporting documentation for payment. Determination of satisfactory completion of the Scope of Work will be based on an overall assessment of the progress Grantee has made towards achieving the goals of the Agreement and the performance measures.

All authorized obligations incurred in the performance of the terms of this Agreement must be reported to the City within 30 days following the completion or termination of this Agreement. No claims submitted after the 30-day period will be recognized as binding upon the City for payment. Any obligations and/or debts incurred by Grantee and not reported to the City within the 30-day period become the sole liability of Grantee, and the City shall be relieved of any and all responsibilities.

6. Prompt Payment

This Agreement is subject to the Prompt Payment Ordinance codified in Chapter 2.06 of the Oakland Municipal Code. Under said Ordinance, the City must disburse Grant funds to Grantee within 20 business days after receipt of an undisputed request for payment. An undisputed request for payment is a request for payment that is not a "disputed invoice" within the meaning of the Prompt Payment Ordinance. Under the Ordinance, a "disputed invoice" is an invoice or request for payment that is either (1) improperly executed by Grantee, (2) contains errors, (3) requires additional evidence to determine its validity, and/or (4) contains expenditures or proposed expenditures that are ineligible or that do not otherwise comply with reimbursement or disbursal requirements of the City or another grant funding source. If a request for payment is "disputed", the payment/disbursal shall not be subject to late penalties until the dispute is resolved. In the event a request for payment is disputed, the City shall notify Grantee and the City's Liaison (as defined in the Prompt Payment Ordinance) in writing within five business days of receiving the disputed request for payment that there is a bona fide dispute, in which case the City shall withhold the disputed amount

and may withhold the full amount if the funding source for the Grant requires that the disputed expenditures be fully resolved prior to any disbursement of Grant funds. If the funding source for the Grant requires its review and approval before payments are made to Grantee, this period shall be suspended for any period of review by said agency. If any amount due by the City to be disbursed to Grantee pursuant to this Agreement is not timely paid in accordance with the Prompt Payment Ordinance, Grantee is entitled to interest penalty in the amount of 10% of the improperly withheld amount per year for every month that payment is not made, provided that Grantee agrees to release the City from any and all further claims for interest penalties that may be claimed or collected on the amount due and paid. Grant recipients that receive interest penalties for late payment pursuant to the Prompt Payment Ordinance may not seek further interest penalties on the same late payment in law or equity.

The Prompt Payment Ordinance further requires that, unless specific exemptions apply, Grantee shall pay undisputed invoices of its subcontractors for goods and/or services within 20 business days of submission of invoices unless Grantee notifies the City's Liaison in writing within five business days that there is a bona fide dispute between Grantee and claimant, in which case Grantee may withhold the disputed amount but shall pay the undisputed amount. Disputed payments are subject to investigation by the City's Liaison and, and upon the filing of a compliant, Grantee, if opposing payment, shall provide security in the form of cash, certified check or bond to cover the disputed amount and penalty during the investigation. If Grantee fails or refuses to deposit security, the City will withhold an amount sufficient to cover the claim from the next Grant payment. The City, upon a determination that an undisputed invoice or payment is late, will release security deposits or withholds directly to claimants for valid claims. Grantee is not allowed to retain monies from subcontractor payments for goods as project retention, and is required to release subcontractor project retention in proportion to the subcontractor services rendered, for which payment is due and undisputed, within five business days of payment. For the purpose of posting on the City's website, Grantee is required to file notice with the City of release of retention and payment of mobilization fees, within five business days of such payment or release; and Grantee is required to file an affidavit, under penalty of perjury, that he or she has paid all subcontractors, within five business days following receipt of payment from the City. The affidavit shall provide the names and address of all subcontractors and the amount paid to each.

7. Evaluation, Monitoring and Reporting

Grantee shall be monitored and evaluated by the City in terms of its effectiveness and timely compliance with the provisions of this Agreement and the effective and efficient achievement of the Scope of Work. Grantee shall undertake continuous quantitative and qualitative evaluation of the Scope of Work as specified in this Agreement and shall make written reports on the results of such evaluation to the Project Manager as reasonably requested by the Project Manager.

In addition to the financial requirements described elsewhere in this Agreement, Grantee agrees that authorized representatives of the City may perform fiscal monitoring of Grantee's record-keeping and reporting to assure compliance with this Agreement.

Grantee also agrees to be bound and abide by the City's Surveillance Ordinance, Oakland Municipal Code Chapter 9.64, including submission of a Use Policy and Impact Statement for the Camera System that is approved by the Privacy Advisory Commission and the Oakland City Council. Additionally, the Ordinance requires submission of an Annual Surveillance Report. As defined in Chapter 9.64, an Annual Surveillance Report means a written report concerning the grant funded Camera program, that includes all of the following:

a. A description of how the Camera program was used, including the number of cameras purchased, Recipient businesses contracted with, and locations of security cameras on business premises;
b. Whether and how often data acquired by the use of the Camera program was directly shared with the City, the name of the Recipient business sharing the data, the types of data disclosed, under what legal standards the information was disclosed and the justification for the disclosures;
c. Where applicable, a breakdown of what physical objects the Camera program hardware was installed upon, using general terms so as not to disclose the specific location of such hardware; and for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
d. Where applicable, a breakdown of where the surveillance technology was deployed geographically in the relevant year;
e. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. This analysis shall also include the race of each person subjected to the technology unless this requirement is waived by the City's Privacy Advisory Commission. If waiver is granted, the annual report will include the written findings in support of this determination;
f. The results of any internal audits, any information about violations or potential violations of the Camera program Use Policy, and any actions taken in response unless the release of such information is prohibited by law; and
g. Information about any data breaches or other unauthorized access to the data collected by the Camera program, including information about the scope of the breach and the actions taken in response.
h. Information, including crime and/or illegal dumping statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
i. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
j. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
k. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request. Grantee agrees that should the City find that a violation of Chapter 9.64

has occurred, Grantee will either return the camera equipment or reimburse the City for the cost.

8. Program Income

Any funds received as return of costs or as income generated from activities funded by this Agreement are the property of the City and must be transmitted to the City promptly.

9. Proprietary or Confidential Information of the City

Grantee understands and agrees that, in the performance of the work or services under this Agreement or in contemplation thereof, Grantee may have access to private or confidential information which may be owned or controlled by the City and that such information may contain proprietary or confidential details, the disclosure of which to third parties may be damaging to the City. Grantee agrees that all information disclosed by the City to Grantee shall be held in confidence and used only in performance of the Agreement. Grantee shall exercise the same standard of care to protect such information as a reasonably prudent Grantee would use to protect its own proprietary data.

10. Records and Audit

Grantee must maintain (a) a full set of accounting records in accordance with generally accepted accounting principles and procedures for all funds received under this Agreement, and (b) full and complete documentation of performance related matters such as benchmarks and deliverables associated with this Agreement. Grantee agrees to comply with all audit, inspection, record-keeping and fiscal reporting requirements mandated by the City, and all state and/or federal audit requirements applicable to the funding sources of the Grant. The City shall notify the Grantee of any records it deems in its reasonable judgment to be insufficient. Grantee shall have 15 calendar days from such notice to correct any specified deficiency in the records, or, if more than 15 days shall be reasonably necessary to correct the deficiency, Grantee shall begin to correct the deficiency within 15 days and correct the deficiency as soon as reasonably possible. Grantee must maintain such records for a period of four years following the last fiscal year during which the City paid an invoice to Grantee under this Agreement.

Grantee must make available at Grantee's office for examination at reasonable intervals and during normal business hours to the City's representatives, as well as representatives of agencies providing funding for the Grant, all books, accounts, reports, files, financial records, and other papers or property with respect to all matters covered by this Agreement, as well as the financial condition of Grantee in general, and shall permit these representatives to audit, examine, and make copies, excerpts or transcripts from such records. The City's representatives may make audits of any conditions relating to this Agreement, as well as the financial condition of Grantee in general, throughout the term of this Agreement and for three years following the expiration of the term of this Agreement.

11. Fraud, Waste and Abuse

Grantee must immediately inform the City of any information or complaints involving criminal fraud, waste, abuse, or other criminal activity in connection with the Work.

12. Compliance with Federal Standards

Not Applicable.

13. Assignment and Subcontracting

Grantee may not assign, subcontract, or otherwise transfer any rights, duties, obligations or interest in this Grant or Agreement or arising hereunder to any person, persons, entity or entities whatsoever without the prior written consent of the City, and any attempt to assign, subcontract, or transfer without such prior written consent shall be void. Consent to any single assignment, subcontract, or transfer shall not constitute consent to any further assignment, subcontract or transfer.

14. Publicity

Any publicity generated by Grantee for the program funded pursuant to this Agreement, during the term of this Agreement or for one year thereafter, shall make reference to the contribution of the City in making the project possible. The words "City of Oakland" shall be explicitly stated in all pieces of publicity, including but not limited to flyers, press releases, posters, brochures, public service announcements, interviews and newspaper articles.

City staff will be available whenever possible at the request of Grantee to assist Grantee in generating publicity for the program funded pursuant to this Agreement. Grantee further agrees to cooperate with authorized City officials and staff in any City-generated publicity or promotional activities undertaken with respect to this program.

15. Insurance

Unless a written waiver is obtained from the City's Risk Manager, Grantee must provide the insurance listed in the City of Oakland **Insurance Requirements** attached hereto as **Schedule Q** and incorporated herein by reference.

16. Indemnification

a. Notwithstanding any other provision of this Agreement, Grantee shall indemnify and hold harmless (and at City's request, defend) the City, and its Councilmembers, officers, partners, agents, and employees (each of which persons and organizations are referred to collectively herein as "Indemnitees" or individually as "Indemnitee") from and against any and all liabilities, claims, lawsuits, losses, damages, demands, debts, liens, costs, judgments, obligations, administrative or regulatory fines or penalties, actions or causes

of action, and expenses (including reasonable attorneys' fees) caused by or arising out of any:

(i) Breach of Grantee's obligations, representations or warranties under this Agreement;
(ii) Act or failure to act in the course of performance by Grantee under this Agreement;
(iii) Negligent or willful acts or omissions in the course of performance by Grantee under this Agreement;
(iv) Claim for personal injury (including death) or property damage to the extent based on the strict liability or caused by any negligent act, error or omission of Grantee;
(v) Unauthorized use or disclosure by Grantee of confidential information; or
(vi) Claim of infringement or alleged violation of any United States patent right or copyright, trade secret, trade mark, or service mark or other proprietary or intellectual property rights of any third party.

b. For purposes of the preceding subsections (i) through (vi), the term "Grantee" includes Grantee, its officers, directors, employees, representatives, agents, servants, sub-consultants and subgrantees.

c. The City shall give Grantee prompt written notice of any such claim of loss or damage and shall cooperate with Grantee, in the defense and all related settlement negotiations to the extent that cooperation does not conflict with City's interests.

d. Notwithstanding the foregoing, the City shall have the right if Grantee fails or refuses to defend the City with counsel acceptable to the City to engage its own counsel for the purposes of participating in the defense. In addition, the City shall have the right to withhold any payments due Grantee in the amount of anticipated defense costs plus additional reasonable amounts as security for Grantee's obligations under this section. In no event shall Grantee agree to the settlement of any claim described herein without the prior written consent of the City.

e. Grantee acknowledges and agrees that it has an immediate and independent obligation to indemnify and defend Indemnitees from any claim or action which potentially falls within this indemnification provision, which obligation shall arise at the time such claim is tendered to Grantee by the City and continues at all times thereafter, without regard to any alleged or actual contributory negligence of any Indemnitee. Notwithstanding anything to the contrary contained herein, Grantee's liability under this Agreement shall not apply to any action or claim arising from the sole negligence, active negligence, or willful misconduct of an Indemnitee.

f. All of Grantee's obligations under this section are intended to apply to the fullest extent permitted by law (including without limitation, California Civil Code Section 2782) and shall survive the expiration or sooner termination of this Agreement.

g. The indemnity set forth in this section shall not be limited by the City's insurance requirements contained in Schedule Q hereof, or by any other provision of this Agreement. The City's liability under this Agreement shall be limited to payment of Grantee in accord to the terms and conditions under this Agreement and shall exclude any liability whatsoever for consequential or indirect damages even if such damages are foreseeable.

17. Non-Liability of City

No member, official, officer, director, employee, or agent of the City shall be liable to Grantee for any obligation created under the terms of this Agreement except in the case of actual fraud or willful misconduct by such person.

18. Right to Offset Claims for Money

All claims for money due or to become due from the City shall be subject to deduction or offset by the City from any monies due Grantee by reason of any claim or counterclaim arising out of this Agreement, any purchase order, or any other transaction with Grantee.

19. Events of Default and Remedies

The occurrence of any of the following shall constitute a material default and breach of this Agreement by Grantee:

a. Failure to adequately perform the Work set forth in the Scope of Work;
b. Improper use or reporting of funds provided under this Agreement by Grantee or its employees or agents;
c. Substantial failure by Grantee to observe and perform any other provision of this Agreement; or
d. Grantee's (1) filing for bankruptcy, dissolution, or reorganization, or failure to obtain a full dismissal of any such involuntary filing brought by another party before the earlier of final relief or 60 days after the filing; (2) making a general assignment for the benefit of creditors; (3) applying for the appointment of a receiver, trustee, custodian, or liquidator, or failure to obtain a full dismissal of any such involuntary application brought by another party before the earlier of final relief or 60 days after the filing; (4) insolvency; or (5) failure, inability or admission in writing of its inability to pay its debts as they become due.

The City shall give written notice to Grantee or Grantee's agent of any default by specifying (a) the nature of the event or deficiency giving rise to the default, (b) the action required to cure the deficiency, if an action to cure is possible, and (c) a date, which shall be not less than 30 calendar days from the mailing of the notice, by which such action to cure, if a cure is possible, must be undertaken. Grantee shall not be in default if Grantee cures such default within the specified cure period, or, if such default is not reasonably capable of cure within the specified period, Grantee begins to cure the default within the cure period and thereafter diligently pursues the cure to completion. Following any notice of an event of default, the

City may suspend payments under this Agreement pending Grantee's cure of the specified breach. Upon an event of default that has not been cured by Grantee, the City, in its discretion, may take any of the following actions:

(A) Terminate this Agreement in whole or in part;
(B) Suspend payments under this Agreement;
(C) Demand immediate reimbursement of any funds disbursed under this Agreement;
(D) Bring an action for equitable relief (a) seeking the specific performance by Grantee of the terms and conditions of the Agreement, and/or (b) enjoining, abating, or preventing any violation of said terms and conditions, and/or (c) seeking declaratory relief;
(E) Bar Grantee from future funding by the City; and/or
(F) Pursue any other remedy allowed at law or in equity.

Unless otherwise terminated as provided in this Agreement, this Agreement will terminate on upon total grant disbursement and/or use, or upon either party's 30-day written notice.

20. Termination or Modification for Lack of Appropriation

The City's obligations under this Agreement are contingent upon the availability of funds from the funding source for this Grant. The City may terminate this Agreement on 30 days' written notice to Grantee without further obligation if said funding is withdrawn or otherwise becomes unavailable for continued funding of the Work.

21. Litigation and Pending Disputes

Grantee shall promptly give notice in writing to the City of any litigation pending or threatened against Grantee in which the amount claimed is in excess of $50,000. Grantee shall disclose, and represents that it has disclosed, any and all pending disputes with the City prior to execution of this Agreement on **Schedule K**, incorporated herein by reference. Failure to disclose pending disputes prior to execution of this Agreement shall be a basis for termination of this Agreement.

22. Conflict of Interest

a. Grantee certifies that no member, officer, or employee of the City or its designees or agents, and no other public official of the City who exercises any functions or responsibilities with respect to the programs or projects covered by this Agreement, shall have any interest, direct or indirect in this Agreement, or in its proceeds during his/her tenure or for one year thereafter.

b. Grantee warrants and represents, to the best of its present knowledge, that no public official or employee of City who has been involved in the making of this Agreement, or who is a member of a City board or commission which has been involved in the making of this Agreement whether in an advisory or decision-

making capacity, has or will receive a direct or indirect financial interest in this Agreement in violation of the rules contained in California Government Code Section 1090 et seq., pertaining to conflicts of interest in public contracting. Grantee shall exercise due diligence to ensure that no such official will receive such an interest.

c. Grantee further warrants and represents, to the best of its present knowledge and excepting any written disclosures as to these matter already made by Grantee to City, that (1) no public official of City who has participated in decision-making concerning this Agreement or has used his or her official position to influence decisions regarding this Agreement, has an economic interest in Grantee or this Agreement, and (2) this Agreement will not have a direct or indirect financial effect on said official, the official's spouse or dependent children, or any of the official's economic interests. For purposes of this paragraph, an official is deemed to have an "economic interest" in (a) any for-profit business entity in which the official has a direct or indirect investment worth $2,000 or more, (b) any real property in which the official has a direct or indirect interest worth $2,000 or more, (c) any for-profit business entity in which the official is a director, officer, partner, trustee, employee or manager, or (d) any source of income or donors of gifts to the official (including nonprofit entities) if the income totaled more than $500, or value of the gift totaled more than $500 the previous year. Grantee agrees to promptly disclose to the City in writing any information it may receive concerning any such potential conflict of interest. Grantee's attention is directed to the conflict of interest rules applicable to governmental decision-making contained in the Political Reform Act (California Government Code Section 87100 et seq.) and its implementing regulations (California Code of Regulations, Title 2, Section 18700 et seq.).

d. Grantee shall incorporate or cause to be incorporated into all subcontracts for work to be performed under this Agreement a provision governing conflict of interest in substantially the same form set forth herein.

e. Nothing herein is intended to waive any applicable federal, state or local conflict of interest law or regulation.

f. In addition to the rights and remedies otherwise available to the City under this Agreement and under federal, state and local law, Grantee understands and agrees that, if the City reasonably determines that Grantee has failed to make a good faith effort to avoid an improper conflict of interest situation or is responsible for the conflict situation, the City may (1) suspend payments under this Agreement, (2) terminate this Agreement, and/or (3) require reimbursement by Grantee to the City of any amounts disbursed under this Agreement. In addition, the City may suspend payments or terminate this Agreement whether or not Grantee is responsible for the conflict of interest situation.

23. Non-Discrimination/Equal Employment Practices

Grantee shall not discriminate or permit discrimination against any person or group of persons in any manner prohibited by federal, state or local laws. During the performance of this Agreement, Grantee agrees as follows:

a. Grantee and Grantee's subgrantees, if any, shall not discriminate against any employee or applicant for employment because of actual or perceived age, marital or familial status, religion, gender, gender identity, gender expression, sexual orientation, race, creed, color, genetic information, ancestry national origin, physical or mental disability including Acquired-Immune Deficiency Syndrome (AIDS) or AIDS-Related Complex (ARC), or military status. This nondiscrimination policy shall include, but not be limited to, the following: employment, upgrading, failure to promote, demotion or transfer, recruitment advertising, layoffs, termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

b. Grantee and Grantee's subgrantees shall state in all solicitations or advertisements for employees placed by or on behalf of Grantee that all qualified applicants will receive consideration for employment without regard to actual or perceived age, marital or familial status, religion, gender, gender identity, gender expression, sexual orientation, race, creed, color, genetic information, ancestry, national origin, physical or mental disability including Acquired-Immune Deficiency Syndrome (AIDS) or AIDS-Related Complex (ARC), or military status.

c. Grantee shall make its goods, services, and facilities accessible to people with disabilities and shall verify compliance with the Americans with Disabilities Act by executing **Schedule C-1**, Declaration of Compliance with the Americans with Disabilities Act, attached hereto and incorporated herein.

d. If applicable, Grantee will send to each labor union or representative of workers with whom Grantee has a collective bargaining agreement or contract or understanding, a notice advising the labor union or workers' representative of Grantee's commitments under this nondiscrimination clause and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

24. Local/Small Local Enterprise Participation

The City has established requirements for participation by local and small local enterprises, including local nonprofit organizations and small local nonprofit organizations, in publicly-supported projects. Unless otherwise indicated, the City acknowledges that Grantee complies with this requirement.

25. Living Wage Requirements

Grantee will be considered a City Financial Assistance Recipient ("CFAR") and must comply with the Oakland Living Wage Ordinance if it receives $100,000 or more in financial assistance from the City during a 12-month period. The Living Wage Ordinance requires that nothing less than a prescribed minimum level of compensation (a living wage) be paid to employees of CFARs (OMC 2.28, Ord. 1250 § 1, 1998). The Ordinance also requires submission of the Declaration of Compliance attached and incorporated herein as **Schedule N** and made part of this Agreement, and, unless specific exemptions apply or a waiver is granted, that Grantee provide the following to its employees who perform services under or related to this Agreement:

a. Minimum compensation – Said employees shall be paid an initial hourly wage rate of **$14.98 with health benefits and $17.19 without health benefits**. These initial rates shall be upwardly adjusted each year no later than April 1 in proportion to the increase at the immediately preceding December 31 over the year earlier level of the Bay Region Consumer Price Index as published by the Bureau of Labor Statistics, U.S. Department of Labor. Effective July 1st of each year, Grantee shall pay adjusted wage rates.

b. Health benefits – Said full-time and part-time employees paid at the lower living wage rate shall be provided health benefits of at least $2.21 per hour. Grantee shall provide proof that health benefits are in effect for those employees no later than 30 days after execution of the contract or receipt of City financial assistance.

c. Compensated days off – Said employees shall be entitled to twelve compensated days off per year for sick leave, vacation or personal necessity at the employee's request, and ten uncompensated days off per year for sick leave. Employees shall accrue one compensated day off per month of full time employment. Part-time employees shall accrue compensated days off in increments proportional to that accrued by full-time employees. The employees shall be eligible to use accrued days off after the first six months of employment or consistent with company policy, whichever is sooner. Paid holidays, consistent with established employer policy, may be counted toward provision of the required 12 compensated days off. Ten uncompensated days off shall be made available, as needed, for personal or immediate family illness after the employee has exhausted his or her accrued compensated days off for that year.

d. Federal Earned Income Credit (EIC) – Grantee shall inform employees that he or she may be eligible for EIC and shall provide forms to apply for advance EIC payments to eligible employees.

e. Grantee shall provide to all employees and to the Office of Contract Compliance, written notice of its obligation to eligible employees under the City's Living Wage requirements. Said notice shall be posted prominently in communal areas of the work site(s) and shall include the above-referenced information.

f. Grantee shall provide all written notices and forms required above in English, Spanish or other languages spoken by a significant number of employees within 30 days of employment under this Agreement.

g. Reporting – Grantee shall maintain a listing of the name, address, hire date, occupation classification, rate of pay and benefits for each of its employees. Grantee shall provide a copy of said list to the Office of Contract Compliance, on a quarterly basis, by March 31, June 30, September 30 and December 31 for the applicable compliance period. Failure to provide said list within five days of the due date will result in liquidated damages of five hundred dollars ($500.00) for each day that the list remains outstanding. Grantee shall maintain employee payroll and related records for a period of four (4) years after expiration of the compliance period.

h. Grantee shall require subgrantees that provide services under or related to this Agreement to comply with the above Living Wage provisions. Grantee shall include the above-referenced sections in its subcontracts. Copies of said subcontracts shall be submitted to the Office of Contract Compliance.

26. Equal Benefits Ordinance

This Agreement is subject to the Equal Benefits Ordinance codified in Chapter 2.32 of the Oakland Municipal Code and its implementing regulations. The purpose of this Ordinance is to protect and further the public, health, safety, convenience, comfort, property and general welfare by requiring that public funds be expended in a manner so as to prohibit discrimination in the provision of employee benefits by City grantees between employees with spouses and employees with domestic partners, and/or between domestic partners and spouses of such employees.

The Ordinance shall only apply to those portions of a Grantee's operations that occur (1) within the City of Oakland; (2) on real property outside the City of Oakland if the property is owned by the City or if the City has a right to occupy the property, and if the contract's presence at that location is connected to a contract with the City; and (3) elsewhere in the United States where work related to a City contract is being performed. The requirements of this chapter shall not apply to subcontracts or subgrantees of Grantee.

The Equal Benefits Ordinance requires, among other things, submission of the Equal Benefits Declaration of Nondiscrimination attached hereto as **Schedule N-1** and incorporated herein by reference.

27. Minimum Wage Ordinance

Oakland employers are subject to Oakland's Minimum Wage Law, whereby Oakland employees must be paid the current Minimum Wage rate.

Employers must notify employees of the annually adjusted rates by each December 15th and prominently display notices at the job site.

The law requires paid sick leave for employees and payment of service charges collected for their services.

28. Political Prohibition

Subject to applicable State and Federal laws, moneys paid pursuant to this Agreement shall not be used for political purposes, sponsoring or conducting candidate's meetings, engaging in voter registration activity, nor for publicity or propaganda purposes designed to support or defeat legislation pending before federal, state or local government.

29. Religious Prohibition

There shall be no religious worship, instruction, or proselytization as part of, or in connection with the performance of the Agreement.

30. Business Tax Certificate or Exemption

Grantee shall obtain and provide proof of a valid City business tax certificate or business tax exemption certificate. Said certificate must remain valid during the duration of this Agreement.

31. Abandonment of Grant

The City may abandon or indefinitely postpone the Grant at any time. Should the Grant be abandoned, the City shall pay Grantee for all services performed thereto in accordance with the terms of this Agreement.

32. Relationship of Parties

The relationship of the City and Grantee is solely that of a grantor and grantee of funds, and should not be construed as a joint venture, equity venture, partnership, or any other relationship. The City does not undertake or assume any responsibility or duty to Grantee (except as provided for herein) or to any third party with respect to the Work performed under this Agreement. Except as the City may specify in writing, Grantee has no authority to act as an agent of the City or to bind the City to any obligation.

33. Warranties

Grantee represents and warrants: (1) that it has access to professional advice and support to the extent necessary to enable Grantee to fully comply with the terms of this Agreement and otherwise carry out the Work; (2) that it is duly organized, validly existing and in good standing under the laws of the State of California; (3) that it has the full power and authority to undertake the Work; (4) that there are no pending of threatened actions or proceedings before any court or administrative agency which may substantially affect the financial condition or operation of the Grantee, other than those already disclosed to the City; and (5) that the persons executing and delivering this Agreement are authorized to execute and deliver such document on behalf of Grantee.

34. Unavoidable Delay in Performance

The time for performance of provisions of this Agreement by either party shall be extended for a period equal to the period of any delay directly affecting this Agreement which is caused by: war; insurrection; strikes; lock-outs; riots; floods; earthquakes; fires; casualties; acts of God; acts of a public enemy; epidemics; quarantine restrictions; freight embargoes; lack of transportation; suits filed by third parties concerning or arising out of this Agreement; or unseasonable weather conditions. An extension of time for any of the above-specified causes will be deemed granted only if written notice by the party claiming such extension is sent to the other party within ten calendar days from the commencement of the cause. Times of performance under this Agreement may also be extended for any cause for any period of time by the mutual written agreement of the City and Grantee.

35. Validity of Contracts

This Agreement shall not be binding or of any force or effect until it is approved for form and legality by the Office of the City Attorney and signed by the City Administrator or his or her designee.

36. Governing Law

This Agreement shall be interpreted under and be governed by the laws of the State of California, except for those provisions relating to choice of law or those provisions preempted by federal law or expressly governed by federal law.

37. Notice

If either party shall desire or be required to give notice to the other, such notice shall be given in writing, via facsimile and concurrently by prepaid U.S. certified or registered postage, addressed to recipient as follows:

City
City of Oakland
Economic and Workforce Development Department
250 Frank Ogawa Plaza, Suite 5313
Oakland, CA 94612
Attn:

Grantee
TBD

Any party to this Agreement may change the name or address of representatives for purpose of this Notice paragraph by providing written notice to all other parties ten (10) business days before the change is effective.

38. Entire Agreement of the Parties

This Agreement supersedes any and all agreements, either oral or written, between the parties with respect to this Grant and contains all of the representations, covenants and agreements between the parties with respect to the Grant. Each party to this Agreement acknowledges that no representations, inducements, promises or agreements, orally or otherwise, have been made by any party, or anyone acting on behalf of any party which are not contained in this Agreement, and that no other agreement, statement or promise not contained in this Agreement will be valid or binding.

39. Amendments and Modifications

Any amendment to or modification of this Agreement will be effective only if it is in a writing signed by all parties to this Agreement.

40. Waiver

Any waiver by the City of an obligation in this Agreement must be in writing and must be executed by an authorized agent of the City. No waiver should be implied from any delay or failure by the City to take action on any breach or event of default of Grantee or to pursue any remedy allowed under this Agreement or applicable law. Any extension of time granted to Grantee to perform any obligation under this Agreement will not operate as a waiver or release from any of its obligations under this Agreement. Consent by the City to any act or omission by Grantee should not be construed to be a consent to any other act or omission or to waive the requirement for the City's written consent to future waivers.

41. Other Agreements

Grantee represents that it has not entered into any agreements that are inconsistent with the terms of this Agreement. Grantee may not enter into any agreements that are inconsistent with the terms of this Agreement without an express written waiver by the City.

42. Severability/Partial Invalidity

If any term or provision of this Agreement, or the application of any term or provision of this Agreement to a particular situation, shall be finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then notwithstanding such determination, such term or provision shall remain in force and effect to the extent allowed by such ruling and all other terms and provisions of this Agreement or the application of this Agreement to other situation shall remain in full force and effect.

Notwithstanding the foregoing, if any material term or provision of this Agreement or the application of such material term or condition to a particular situation is finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then the parties hereto agree to work in good faith and fully cooperate with each other to amend this Agreement to carry out its intent.

43. Commencement, Completion and Close-out

It shall be the responsibility of Grantee to coordinate and schedule the Work to be performed so that commencement and completion take place in accordance with the provisions of this Agreement. Any time extension granted to Grantee to enable Grantee to complete the Work must be in writing and shall not constitute a waiver of rights the City may have under this Agreement. Should Grantee not complete the Work by the scheduled date or by an extended date, the City shall be released from all of its obligations under this Agreement.

Within thirty (30) days of completion of the performance under this Agreement, Grantee shall make a determination of any and all final costs due under this Agreement and shall submit a requisition for such final and complete payment (including without limitations any and all claims relating to or arising from this Agreement) to the City. Failure of Grantee to timely submit a complete and accurate requisition for final payment shall relieve the City of any further obligations under this Agreement, including without limitation any obligation for payment of work performed or payment of claims by Grantee.

44. Consents and Approvals

Any consent or approval required under this Agreement may not be unreasonably withheld, delayed, or conditioned.

45. Inconsistency

If there is any inconsistency between the main agreement and the attachments/exhibits, the text of the main agreement shall prevail.

46. Counterparts

This Agreement may be signed in multiple counterparts, which, when signed by all parties, will constitute a binding agreement.

47. Exhibits

The following exhibits and schedules are attached to this Agreement and are hereby incorporated herein by reference:

Schedule A:	Scope of Work and Budget
Schedule C-1:	Compliance with ADA
Schedule K:	Pending Dispute Disclosure Form
Schedule N:	Declaration of Compliance with Living Wage
Schedule N-1:	Equal Benefits, Declaration of Nondiscrimination
Schedule Q:	Insurance Requirements

48. Approval

If the terms of this Agreement are acceptable to Grantee and the City, sign and date below.

[SIGNATURES ON NEXT PAGE]

"CITY"

CITY OF OAKLAND, a municipal corporation

By: _____
City Administrator (date)

Approved for forwarding:

By:_____
Department Head (date)

_____
Resolution Number

Approved as to form and legality:

By:_____
Deputy City Attorney

"GRANTEE"

By: _____

Name:_____

Title: ____AUTHORIZED OFFICER OF ORGANIZATION____

Date: _____

GRANT AGREEMENT

EXHIBIT A

SCOPE OF WORK AND BUDGET

[Scope of Work to incorporate Use Policy and Impact Analysis, as reviewed and approved by the Privacy Advisory Commission]

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne L. Armstrong
Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Automated License Plate Reader – 2021 Annual Report

DATE: March 22, 2022

Background

Oakland Police Department (OPD) ALPR Policy 430 (430.8 Agency Monitoring and Controls) states that the "ALPR Coordinator shall provide the Chief of Police and Public Safety Committee with an annual report for the previous 12-month period." Policy 430 precedes City Council adoption of the Surveillance Technology Ordinance, enshrined in Oakland Municipal Code (OMC) 9.64; OMC 9.64 separately also requires annual reports as well as review and recommendation of a Surveillance Use Policy (SUP) and Surveillance Impact Report (SIR) – referred to collectively as "Privacy Policy."

The following bullet points outline the history of OPD's presentation of ALPR Privacy Policy documents to the City's Privacy Advisory Commission (PAC):

- January 2019 - Presentation of draft ALPR Privacy Policy.
- February 2019 - Presentation of draft ALPR Privacy Policy.
- April 2019 - Presentation of draft ALPR Privacy.
- January 2021 - Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports.
- February 2021 - Presentation of revised ALPR Privacy Policy; PAC vote to recommend to the City Council that OPD be prohibited from using ALPR technology for two years.
- OPD then presented the ALPR Privacy Policy and 2019 / 2020 Annual Reports to the Public Safety Committee on May 11, and City Council on May 18**.** The City Council was presented with two options – OPD's recommendation to approve the privacy policy as well as the PAC recommendation. The full City Council voted to send the Policy back to the PAC for further review and that OPD provide all missing information.
- August 2021 - Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports.
- October 2021- Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports; PAC commissioners suggest having an ad-hoc meeting but then confirm that there are not enough commissioners who are prepared to hold an ad-hoc meeting.
- November 2021- Presentation of revised ALPR Privacy Policy and 2019 / 2020 Annual Reports – at this meeting the PAC again votes to recommend a two-year moratorium OPD use of ALPR technology.

OPD is preparing to again present its Privacy Policy to the City's Public Safety Committee along with the PAC November 2021 motion for a two-year moratorium at the time of the production of this report.

2021 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Table 1 below shows the total scans and hits by month – the total license plate photographs made and stored each month (1,980,132 stans total for the year). Table 1 also shows the number of times the vehicle-based systems had a match ("hit") with a California Department of Justice (CA DOJ) database (2,503 total for 2021). OPD's very outdated ALPR system can only quantify these two figures; the system can no longer quantify individual queries or perform any audit functions, as the software is no longer supported from the original vendor. Prior, the system could run reports that detailed the reasons for queries (e.g. a type of criminal investigation). OPD can only provide more comprehensive use data if and when a newer ALPR system is acquired.

Table 1: 2021 OPD ALPR Scans and Hits

Month	Year	Scans	Hits
Jan	2021	198,027	235
Feb	2021	145,547	229
Mar	2021	212,367	238
Apr	2021	166,993	146
May	2021	184,147	235
Jun	2021	155,502	135
Jul	2021	98,814	110
Aug	2021	190,136	249
Sep	2021	221,509	375
Oct	2021	161,789	242
Nov	2021	121,565	143
Dec	2021	123,736	166
2021 Totals		**1,980,132**	**2503**

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The Federal Bureau of Investigation (FBI) had access to OPD ALPR data without following the standard data access request protocols outlined in Policy 430.9 "Releasing or Sharing ALPR Data;" OPD has provided this level of access because there is a Council-approved Safe Streets Task Force Memorandum of Understanding (MOU)[1]. OPD believes that the Task Force MOU allowed for ALPR data-sharing with specific FBI agents who have been co-located with OPD in the Police Administration Building and worked on homicide cases. However, OPD personnel ran an audit of ALPR data queries and discovered that there were

[1] The mission of the FBI San Francisco Violent Crimes Safe Streets Task Force MOU is to identify and target for prosecution criminal enterprise groups and individual responsible for crimes of violence such as murder and aggravated assault, as well as other serious crimes. The MOU does not specifically address the sharing of ALPR data; however, the MOU does specifically articulate protocols for data sharing.

no queries from these FBI personnel. OPD has decided to revoke access to FBI these agents as of 9/28/2021 to alleviate concerns over data privacy.

OPD has not received requests for ALPR data in 2021 from outside police agencies.

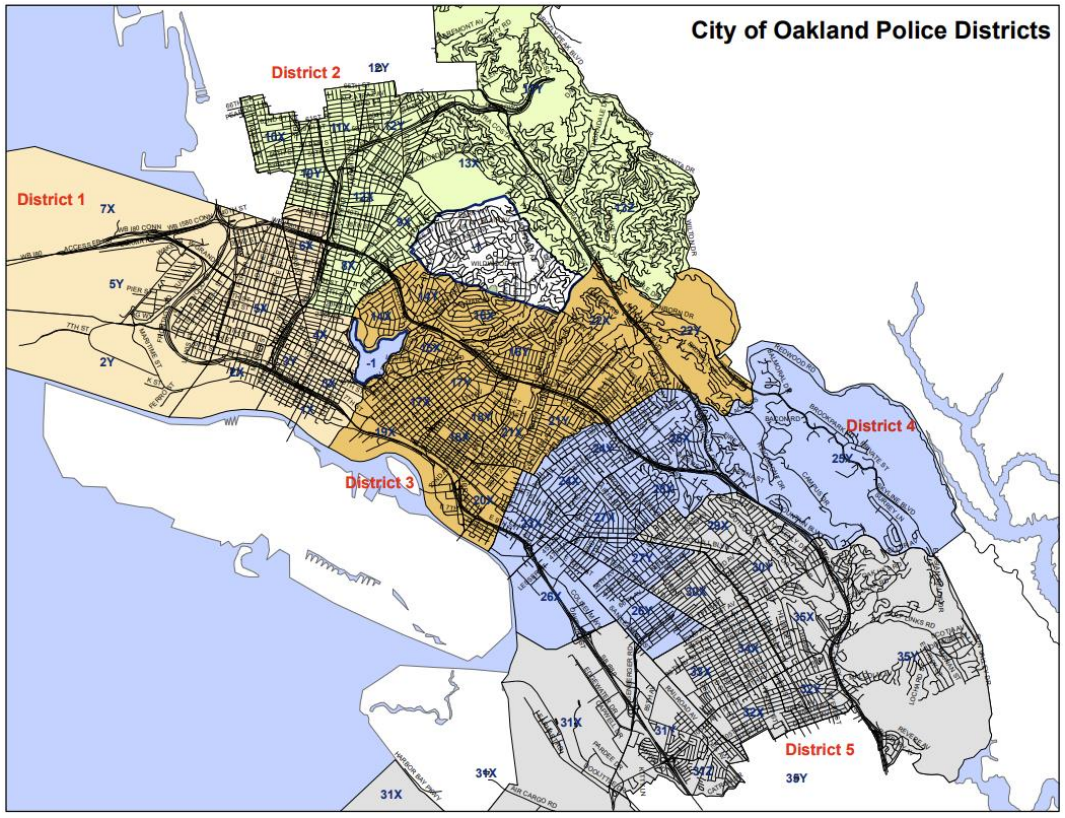
C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The ALPR cameras are installed upon fully marked OPD patrol vehicles (24 operational; 8 inoperable).

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

These vehicles are assigned to the Bureau of Field Operations I (administered out of the Police Administration Building in downtown Oakland) as well as Bureau of Field Operations II (administered from the Eastmont Substation). The vehicles are deployed throughout the City in a patrol function to allow for large areas of the City to have ALPR coverage as the patrol vehicles are used to respond to calls for police service; Figure 1 below is a map showing where patrol vehicles equipped with ALPR are generally deployed throughout the City.

Figure 1: ALPR-Equipped Patrol Vehicle Deployment Distribution



E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Members of the public have spoken at PAC meetings regarding concerns of negative impacts to privacy protections (e.g., that OPD could use ALPR server data to establish travel patterns of particular vehicles associated with particular license plates, and/or that ALPR data can be inadvertently released through inadequate privacy protocols). OPD has also heard comments that more advanced ALPR systems may be used to track other vehicle attributes (e.g., bumper stickers). More recently, OPD staff have also heard from members of the public in support of ALPR systems and wanting to be sure that OPD utilizes technology appropriately to support OPD investigations. Furthermore, OPD personnel are of media reports of ALPR systems where a lack of updates between local systems and State CA DOJ databases lead to inaccurate stolen vehicle notifications, which have led law enforcement to stopping motorists because of stolen vehicle notifications.

OPD is not able to provide the race of each person connected to each ALPR scan. Race data is not captured in the scan itself as explained in the ALPR Draft Surveillance Impact Report. Race data would only be captured if there is a related criminal investigation for a particular ALPR scan capture. Staff could attempt to connect each scan to the associated vehicle registration of each scanned license plate. However, staff would not know if the vehicle driver, at the time of the ALPR scan, is the same person as the registered owner of the vehicle. Furthermore, staff believes that the potential for greater invasiveness in capturing this data outweighs the public benefit of capturing the data. Staff therefore recommend that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The current system is outdated, and the software is not supported from the original vendor. Prior to this loss in function, the system could be used to run reports for sample audits that detailed the reasons for queries (e.g., type of criminal investigation). The ALPR system can currently quantify only hit and scan data as noted in Part A above. OPD currently faces a "Catch-22" situation: OPD cannot produce audits and annual reports that meet the expectations of the Surveillance Technology Ordinance because its current ALPR database and software are outdated and only partially functional. OPD can update the system for approximately $16,000 – but pursuant to the surveillance ordinance, OPD cannot update the system unless the City Council first approves OPD's ALPR Use Policy. The PAC has cited OPD's failure to produce audits and annual reports as a significant reason for the PAC's refusal to support OPD's Use Policy and its continued use of ALPR. Staff wants to comply with all facets of the City's Surveillance Ordinance (OMC 9.64) and continue to bring annual reports to the PAC for ongoing independent oversight of this useful technology, but it cannot do so unless it upgrades its ALPR technology.

OPD created a new ALPR Training document in 2020; OPD staff audited the OPD online training and document review system to ensure that staff completed the ALPR Training module. Approximately 75% of staff have completed the training thus far and OPD is implementing directives to ensure 100% compliance.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The City's Information Technology Department (ITD) confirmed to OPD that they have not detected any ALPR information breaches at the time of OPD's inquiry for the production of this annual report.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 2 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 2: 2021 OPD Type 1 Crime Data

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Additionally, ALPR was used to recover 39 stolen vehicles recovered with a value an estimated value of $227,337. ***Appendix A*** to this report provides additional information about stolen vehicles and/or vehicles involved in carjackings where ALPR played a notification and/or investigatory role.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

OPD has received two new PRRs in 2021 related to ALPR; there were five total open ALPR-related PRRs as of December 31, 2021.

These requests related to the number of ALPR camera systems (see Section C above), ALPR data (the license plate number, date, time, and location information for each license plate recorded for related to either specific license plates or all captured data during certain time periods), and OPD emails related to ALPR data. Other requests related to the sharing of data with other agencies as outlined in Section B above. There are also PRRs relating to technology contracts.

For all ALPR PRRs, OPD can generally provide date and time information. OPD cannot provide information related to locations where license plates were photographed, nor information related to the specific vehicles. Some of these PRRs have been processed and

completed in 2022 during the time of the production of this report – status information below reflects recent updates made in 2022.

No.#	PRR#	Nature of Request	Status	Content Provided
1	*RT 16630*	*All records responsive to the below requests dated from January 1, 2014 through July 28, 2016. - The full documentation of all contracts or non-disclosure agreements (enacted OR IN EFFECT between the above dates) with the companies "Persistent Surveillance Systems" or "Vigilant Solutions" (more of request: https://oaklandca.nextrequest.com/requests/RT-16630.*	*Still being processed*	*n/a*
2	*18-649 –*	*The names of all agencies, organizations and entities with which the Oakland Police department shares Automatic License Plate Reader ("ALPR") data, such as the National Vehicle Location Service; * The names of all agencies and organizations from which the department receives ALPR data; * The names of all agencies and organizations from which the department shares "hot list" information; * The names of all agencies and organizations from which the department receives "hot list" information; more of request: https://oaklandca.nextrequest.com/requests/18-649*	*open*	*OPD ALPR Policy 430: https://oaklandca.nextrequest.com/documents/618507/download*
3	*19-1546*	*How many automated license plate readers the Oakland Police Department has in use currently? Are they in fixed locations or on police cars, or other? How many vehicles on your hotlist currently? What's is the hit rate currently, and what was it in March 2018? How long is this data retained for? Is there a formal data retention limit? Have you shared any of this LPR data with any third parties, including non law enforcement bodies? If so, who? Have you bought license plate data from any third parties, and if so who? Has there been any communication between the department and representatives from*	*Open*	*Content not yet provided*

No.#	PRR#	Nature of Request	Status	Content Provided
		or people acting on behalf of US Immigration and Customs enforcement and / or US Border Patrol? If so, please can you share all correspondence (inc attachments)? More information: https://oaklandca.nextrequest.com/requests/19-1546		
4	*21-6410*	*Requesting ALPR Data for the last two years*	*open*	
5	*21-6660*	*Please provide me with an electronic copy (preferably PDF) of the guidelines and procedures referenced here in OPD's ALPR policy 430 enacted in 2016, including all amendments and revisions thereto: "The Bureau of Services Deputy Chief shall be the administrator of ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq."* *Please provide records from the years 2016-2021.*	*open*	

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Zero; OPD did not incur any maintenance, licensing, or training costs. Training is completed using OPD's online portal as well as staff time.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

OPD and the PAC are developing and reviewing a new ALPR Surveillance Policy contemporaneous to the production of this report for OPD ALPR Use Policy 430.OPD is requesting PAC review and recommendation to City Council of this new Surveillance Use Policy (SUP). This new policy will cover all required areas of OMC 9.64.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

LeRonne L. Armstrong,
Chief of Police

Reviewed by,
Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Carlo Beckman, Police Services Manager
OPD, Research and Planning Section

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Section

David Pullen, Officer
OPD, IT Unit, Bureau of Services

Appendix A

ALPR Stolen or Carjacked Vehicle Data 2021

For all the examples below, officers performed necessary verification of the stolen vehicle status before acting.

1. 21-001682; 01/11/2021 – Officers on patrol had an ALPR hit on the 1600 block of 18th Street. The vehicle was unoccupied and reported carjacked by San Francisco PD. Vehicle was recovered and towed per SFPD's request. Age of data: ~6days
    a. Vehicle Data: 2005 Ford F-150
2. 21-001802; 01/11/2021– Officers on patrol had an ALPR hit on the 200 block of 19th Street. The vehicle was unoccupied and reported stolen by South San Francisco PD. Vehicle was recovered and towed per SSFPD's request. Age of data: ~2 days.
    a. Vehicle Data: 2000 Chevy Tahoe
3. 21-002447; 02/09/2021 – Officers on patrol had an ALPR hit on the 1100 block of E. 15th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~26 days.
    a. Vehicle Data: 1990 Mazda 626 DX/LX
4. 20-056291; 01/17/2021 – Officers on patrol had an ALPR hit on the 1600 block of 8th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~14 months.
    a. Vehicle Data: 2000 Ford Focus
5. 21-002722; 01/18/2021 – Officers on patrol had an ALPR hit on the 1300 block of 5th Street. The vehicle was occupied, and officers attempted to detain the suspects, who fled. The vehicle was reported stolen by Berkeley PD. Age of data: ~2 days
    a. Vehicle Data: 2016 Mazda CX5
6. 21-003887; 01/26/2021 – Officers on patrol had an ALPR hit on the 9700 block of B Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~7 days.
    a. Vehicle Data: 2000 Honda CRV
7. 21-006106; 03/15/2021 – Officers on patrol had an ALPR hit in the area of Fruitvale Ave & Foothill Blvd. The vehicle was occupied, and a stop was conducted. The driver was the registered owner of the vehicle and did not update OPD when they found and recovered the vehicle on 02/08/2021. The driver/registered owner was released. Vehicle was associated with strong-arm robbery, assault & battery, and kidnapping (initially of the victim). Age of data: ~1 month.
    a. Vehicle Data: 2003 Nissan Maxima
8. 21-006112; 02/08/2021 – Officers on patrol had an ALPR hit on the 3800 block of San Leandro Street. The vehicle was reported stolen out of San Leandro PD. The vehicle was unoccupied, and the vehicle was recovered and towed. Age of data: ~10 days.
    a. Vehicle Data: 1998 Nissan Frontier

9. 21-006743; 02/17/2021 – Officers on patrol had an ALPR hit on the 250 block of 7th Street. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was released to them. Age of data: ~6 days.
    a. Vehicle Data: 1999 Ford F-150
10. 21-009814; 03/05/2021 – Officers on patrol had an ALPR hit on the 2800 block of 14th Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was released to a friend of the owner. Age of data: ~3 days.
    a. Vehicle Data: 1991 Honda Civic
11. 21-010933; 03/09/2021 – Officers on patrol had an ALPR hit on the 600 block of 6th Street. The vehicle was occupied, and the individual was detained and arrested. The vehicle was reported stolen out of San Francisco PD and was recovered and towed. Age of data: ~20 days.
    a. Vehicle Data: 2005 Ford Econoline E350
12. 21-0111404; 03/13/2021 – Officers on patrol had an ALPR hit in the area of 45th Ave and E. 12th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~1 day.
    a. Vehicle Data: 2006 Nissan Maxima
13. 21-011572; 03/17/2021 – Officers on patrol had an ALPR hit on the 1300 block of E. 24th Street. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle was recovered and released to the owner. Age of data: ~4 days.
    a. Vehicle Data: 2000 Honda CRV
14. 21-011654; 04/06/2021 – Officers on patrol had an ALPR hit on the 1600 block of Campbell Street. The vehicle was unoccupied, attempts to contact the owner were successful, but the vehicle was disabled, it was recovered and towed. Age of data: ~24 days.
    a. Vehicle Data: 1994 Honda Civic
15. 21-011750; 03/30/2021 – Officers on patrol had an ALPR hit on the 1700 block of Marin Way. The vehicle was occupied, and a stop was conducted, with one individual being arrested for auto-theft. Attempts to contact the owner were unsuccessful, the vehicle was recovered and towed. Age of data: ~17 days
    a. Vehicle Data: 2001 GMC Yukon
16. 21-012745; 04/23/2021 – Officers on patrol had an ALPR hit on the 800 block of Chester Street. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~1 month.
    a. Vehicle Data: 1999 Honda Civic
17. 21-014081; 03/28/2021 – Officers on patrol had an ALPR hit on the 700 block of Wood Street. The vehicle was unoccupied and reported stolen by Hayward PD. The vehicle was recovered and towed. Age of data: ~5 days
    a. Vehicle Data: 1998 Ford Econoline

18. 21-015106; 04/06/2021 – Officers on patrol had an ALPR hit on the 1600 block of 16th Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~3 days.
    a. Vehicle Data: 1989 Toyota Pickup
19. 21-026244; 06/10/2021 – Officers on patrol had an ALPR hit on the 1100 block of Chestnut Street. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~2 days.
    a. Vehicle Data: 2003 Silver Nissan Altima
20. 21-017449; 04/20/2021 – Officers on patrol had an ALPR hit on the 3200 block of Wood Street. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle was recovered and released to the owner. Age of data: ~3 days.
    a. Vehicle Data: 2003 Chevy Silverado
21. 21-018211; 04/25/2021 – Officers on patrol had an ALPR hit on the 3300 block of Helen Street. The vehicle was unoccupied, recovered, and towed. Age of data: ~4 days.
    a. Vehicle Data: 1997 Honda Civic
22. 21-018480; 04/23/2021 – Officers on patrol had an ALPR hit on the 1300 block of 5th Street. The vehicle was occupied, and a stop was initiated. An individual was detained and arrested. Attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~1 day.
    a. Vehicle Data: 1993 Honda Civic
23. 21-020648; 05/08/2021 – Officers on patrol had an ALPR hit on the 2700 block of 10th Avenue. The vehicle was unoccupied and inoperable, the vehicle was recovered and towed. Age of data: ~2 days.
    a. Vehicle Data: 2000 Honda Accord
24. 21-020912; 05/29/2021 – Officers on patrol had an ALPR hit on the 5500 block of Bancroft Avenue. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~22 days
    a. Vehicle Data: 1995 Honda Odyssey
25. 21-035523; 07/31/2021 – Officers on patrol had an ALPR hit on the 2300 block of Embarcadero. The vehicle was moving and occupied, and a stop was conducted. Three suspects were detained with one being arrested for possession of a stolen vehicle. A stolen firearm was also recovered. The vehicle was recovered and released to the owner. Age of data: ~1 day.
    a. Vehicle Data: 2007 White Mercedes CLK
26. 21-025743; 06/12/2021 – Officers on patrol had an ALPR hit on the 550 block of 30th Street. The vehicle was unoccupied, recovered, and towed. Age of data: ~7 days
    a. Vehicle Data: 2003 Mazda Protégé
27. 21-027162; 06/12/2021 – Officers on patrol had an ALPR hit while on the 550 block of 34th Street. The vehicle was confirmed to be reported stolen by Berkeley PD. The vehicle was unoccupied, attempts to contact the owner were successful, the vehicle, however, was inoperable and was recovered and towed. Age of data: ~5 days
    a. Vehicle Data: 1997 Honda Accord

28. 21-027192; 06/12/2021 – Officers on patrol had an ALPR hit on the 550 block of 30th Street. The vehicle was confirmed to be reported stolen by Berkeley PD. The vehicle was unoccupied, recovered, and towed. Age of data: ~11 days
    a. Vehicle Data: 1997 Honda Civic
29. 21-031826; 07/12/2021 – Officers on patrol had an ALPR hit in the area of E. 15th Street and Miller Avenue. The vehicle was occupied and stopped with an individual being detained and arrested. Attempts to contact the owner were successful and the vehicle was recovered and released. Age of data: ~3 days.
    a. Vehicle Data: 1992 Toyota Previa
30. 21-033234; 07/28/2021 – Officers on patrol had an ALPR hit on the 200 block of 11th Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~11 days
    a. Vehicle Data: 2018 Volkswagen Tiguan
31. 21-034757; 09/04/2021 – Officers on patrol had an ALPR hit in the area of 30th Street and Telegraph Avenue. The vehicle was unoccupied, attempts to contact the owner were successful, and the vehicle was recovered and released to the owner. Age of data: ~1 month
    a. Vehicle Data: 1991 Honda Accord
32. 21-036467; 08/23/2021 – Officers on patrol had an ALPR hit on the 1100 block of E. 15th Street. The vehicle (which was carjacked) was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~18 days.
    a. Vehicle Data: 2015 Hyundai Veloster
33. 21-037283; 08/10/2021 – Officers on patrol had an ALPR hit on the 1600 block of 62nd Avenue. The vehicle was reported as being carjacked by BART PD. The vehicle was unoccupied, recovered, and towed. Age of data: ~1 month
    a. Vehicle Data: 2008 Toyota Corolla
34. 21-039386; 08/23/2021 – Officers on patrol had an ALPR hit on the 2200 block of Embarcadero. The vehicle was occupied and stopped with an individual being detained and arrested. Attempts to contact the owner were successful and the vehicle was recovered, but the owner did not show up and the vehicle was towed. Age of data: Recovered same day.
    a. Vehicle Data: 2002 Chevy Silverado 1500
35. 21-040524; 08/29/2021 – Officers on patrol had an ALPR hit on the 3400 block of Elm Street. The vehicle was reported stolen out of Berkeley PD. The vehicle was unoccupied, inoperable, recovered, and towed. Age of data: ~5 days
    a. Vehicle Data: 2002 Dodge RAM 2500
36. 21-044190; 09/20/2021 – Officers on patrol had an ALPR hit in the area of 23rd Avenue and E. 11th Street. The vehicle was occupied and stopped with an individual being detained and arrested. The vehicle was reported stolen out of Emeryville PD. The vehicle was recovered and towed. Age of data: ~1 month
    a. Vehicle Data: 2011 Ford F150

37. 21-049102; 11/01/2021 – Officers on patrol had an ALPR hit on the 4000 block of Brookdale Avenue. The vehicle was unoccupied, attempts to contact the owner were unsuccessful, and the vehicle was recovered and towed. Age of data: ~12 days
    a. Vehicle Data: 2007 Chevy Express Van
38. 21-049863; 10/23/2021 – Officers on patrol had an ALPR hit on the 1200 block of 21st Avenue. The vehicle was reported stolen out of San Jose PD. The vehicle was occupied, and a stop was initiated, with two people being temporarily detained. An investigation discovered that the person who reported the vehicle stolen was not the registered owner and driver and passenger were released without further delay. Age of data: ~4 days
    a. Vehicle Data: 2003 Toyota Corolla
39. 21-051300; 11/01/2021 – Officers on patrol had an ALPR hit on the 4700 block of Bancroft Avenue. The vehicle was reported stolen by the Alameda County Sheriff's Office, was unoccupied, recovered and towed. Age of data: ~5 days.
    a. Vehicle Data: 1993 GMC Sierra

Non-Stolen Vehicle Cases

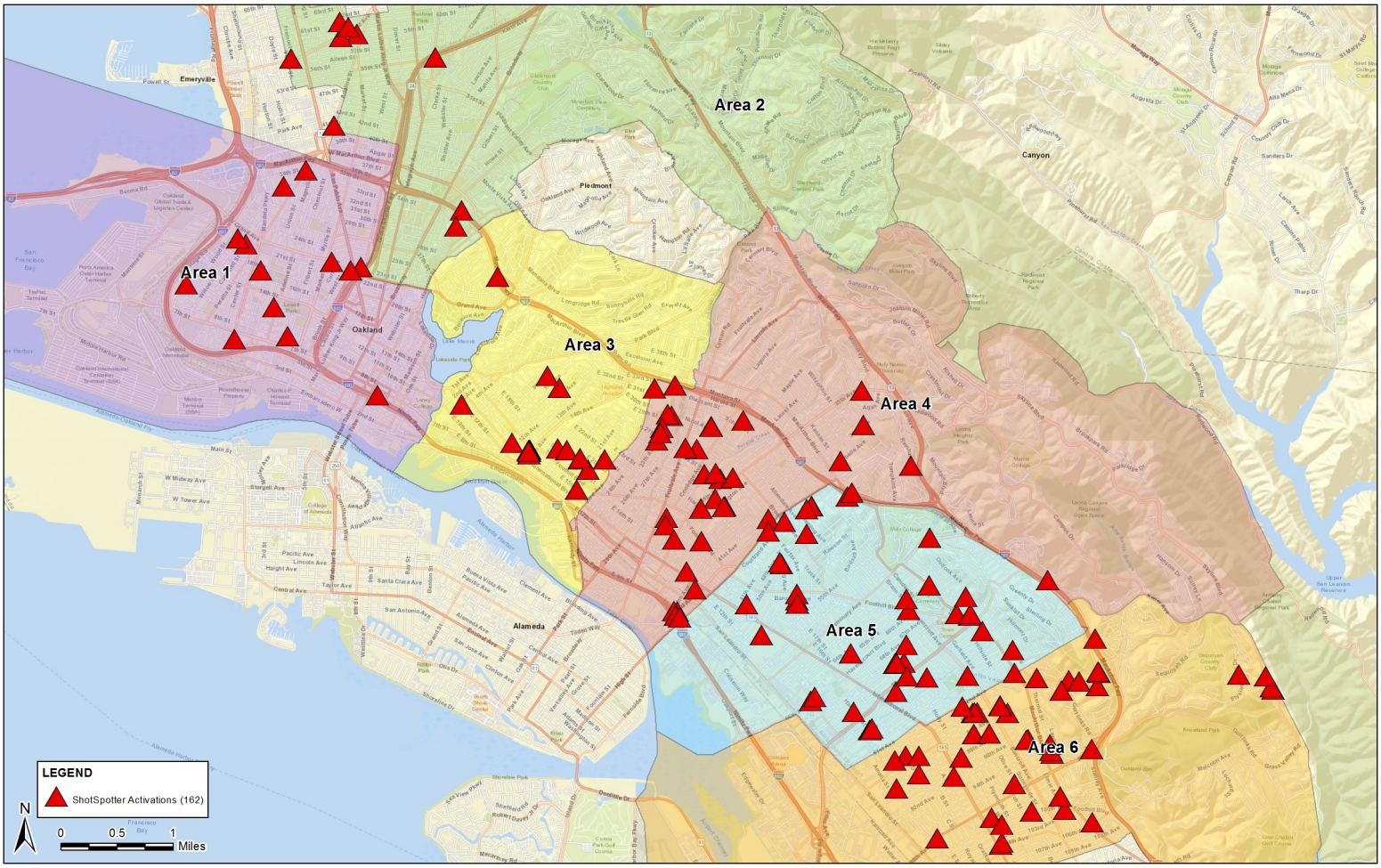
1. 21-012691; 03/19/2021 – ALPR was utilized to capture/scan license plates of vehicles participating in an illegal and unpermitted cabaret event party. Age of Data: Not Applicable
2. 21-012836; 03/20/2021 – ALPR was utilized by Pleasant Hill PD for a vehicle that was involved in an attempted murder. A stop was conducted, and an individual was detained and arrested. An illegal firearm was also recovered. Age of Data: ~6 days
3. 21-014039; 03/29/2021; – Officers on patrol had an ALPR hit on the 700 block of Walker Avenue. The vehicle was unoccupied, but the plate did not match the vehicle VIN it was attached to. The officer removed the plate and turned it into evidence. Age of data: 2 days.
4. 21-025695; 06/05/2021 – ALPR was utilized to search for a car that was suspected of being involved in a shooting. A warrant was obtained, and the individual was arrested. Age of data: ~1 month.
5. 21-031812; 07/09/2021 – Officers on patrol had an ALPR hit on the 7200 block of MacArthur Blvd for a vehicle involved in a robbery. The vehicle was occupied, a stop was attempted, and the suspects fled, eventually evading capture. Age of data: ~1 day.
6. 21-034075; 07/23/2021 – Officers on patrol had an ALPR hit on the 200 block of 29th Street. The vehicle was unoccupied, and the license plate was switched. The license plate was removed and attempts to contact the owner were unsuccessful. The license plate was remanded to evidence. Age of data: ~4 days.

OAKLAND POLICE DEPARTMENT
455 7TH ST., OAKLAND, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly ShotSpotter Activations Report — Citywide

14 Mar. – 21 Mar., 2022

ShotSpotter Activations	Weekly Total	YTD 2021	YTD 2022	YTD % Change 2021 vs. 2022
Citywide	162	2,091	2,003	-4%
Area 1	13	199	217	9%
Area 2	9	58	69	19%
Area 3	19	225	209	-7%
Area 4	36	327	352	8%
Area 5	40	722	575	-20%
Area 6	45	560	581	4%



All data sourced via ShotSpotter Insight.

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne Armstrong, Chief of Police

FROM: Anwawn Jones, Sergeant OPD, Intel Unit

SUBJECT: Cellular Site Simulator – 2021 Annual Report

DATE: February 25, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant these annual report requirements.

Sergeant Anwawn Jones is currently the CSS Program Coordinator.

2021 Data Points

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

The Cell Site Simulator Surveillance (CSS) Impact report explains that, "Cellular site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would a networked tower.

CSS receives signals and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cellular site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others.

The authorized purposes for using CSS interception technology and for collecting information using that technology to:

a. Locate missing persons
b. Locate at-risk individuals
c. Locate victims of mass casualty incidents
d. Assist in investigations involving danger to the life or physical safety of an individual
e. Apprehend fugitives

The technology was requested one time in 2021. The request was part of the investigation into the fugitives involved in the shooting of a retired OPD Captain. The Alameda District Attorney's Office approved the use. However, officers discovered the suspects prior to use of the technology.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know[1], such as an inspector with the District Attorney's Office. However, no CSS data would be downloaded, retained, or shared. No data was generated or shared with any agency because it was not actually used in 2021.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

CSS is not attached to fixed objects.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year.

CSS was not utilized anywhere in the City in 2021.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential

[1] DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

In terms of "an analysis shall also identify the race of each person that was subject to the technology's use":

- *The technology was not used, and therefore there was no data generated from usage;*
- *OPD does have information about the suspect(s) connected to the case that precipitated the technology request. However, the phone related to the considered usage could have been in possession of other people. The phone also could have been registered by a different person and/or registered using a pseudonym contact.*

For the reasons cited above, staff recommends that the PAC waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the possible inaccuracy of the information potentially gathered in this situation.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.

There were no uses in 2021 and thus no need for any audits. There were no policy violations.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no uses in 2021 and thus no possible data breaches.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year.

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates.

There are no existing or new public records request for the 2021 calendar year.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

Zero ($0.00). OPD did not incur any maintenance, licensing, or training costs.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Roland Holmgren, Captain
OPD, Violent Crimes Operations Center

Prepared by:
Anwawn Jones, Sergeant
OPD, Intel Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne Armstrong, Chief of Police

FROM: Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations

SUBJECT: OPD Crime Lab Biometrics DNA Analysis Technology 2021 Annual Report

DATE: March 11, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for approved surveillance technology items (by the Privacy Advisory Commission per OMC 9.64.020 and by City Council per OMC 9.64.030), city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the PAC, city staff shall submit the annual report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; or
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended City Council adoption of the "Oakland Police Department (OPD) Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology Use Policy on October 1, 2020; following the PAC's vote, the City Council adopted Resolution No. 88388 C.M.S. on December 1, 2020. This resolution approved OPD's use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology. OMC 9.64.040 requires that, after City Council approval of surveillance technology, OPD provide an annual report for PAC review before submitting to City Council. This report is intended to serve to comply with this mandate.

2021 Data Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

General Overview

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic

DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

Specifics: How DNA testing was used in 2021

*The Forensic Biology Unit analyzed 430 (**see Attachment A for Case Record IDs**) requests between January 1, 2021 to December 31, 2021. Over 2,300 items of evidence were examined, from which 5,278 samples were subjected to digestion and extraction using the Versa and EZ1 instruments. Scientist subjected 5,425 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 2,196 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with GMIDX or FaSTR and ArmedXpert software.*

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Discovery to the Alameda County District Attorney's Office was provided in 29 cases. A standard discovery packet includes the reports, technical and administrative review sheets, case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The Biometric Use Policy covers the specific technology covered. In general, the digestion, quantitation, normalization/amplification, typing, interpretation and databasing are housed in the laboratory of the Police Administration Building (PAB). Database equipment is located in a secure location elsewhere in the PAB as disclosed in the Use Policy. Currently, no equipment resides outside of these locations.

A cloud-based server location is under evaluation as a replacement for the server in the PAB. The details of this location and security would be handled under the auspices of the City of Oakland ITD policy and procedure and would meet or exceed industry standard for handling of secure servers.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. The laboratory services crimes that occur in all areas of the City of Oakland.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review:

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

The laboratory request for services form does not collect race information. It could be argued that requiring information that is not necessary for analysis, such as race, could be biasing; indeed, it would be a great invasion of privacy to capture this data since it is irrelevant to the analyses performed. Furthermore, the race of individuals subject to the DNA analysis technology's use is not revealed during evaluation of evidence as non-coding regions of DNA are typed and do not contain this information. Therefore, staff recommends that the PAC waive the requirement to identify the race of each person subject to the technology's use and make a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the potential greater invasiveness in capturing such data.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy (SUP), and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

All Forensic Biology personnel and relevant management were required to review and sign that they understood and would abide by the Surveillance Use Policy and the Impact Reports. Under accreditation, the Laboratory actively seeks feedback from its customers and no concerns were conveyed regarding violations or concerns around the SUP. Lastly, the Laboratory has a means to identify risks through Incident Response. Staff are encouraged to participate in Incident Response by filing Incident Alerts where there were concerns. No violations or potential violations were identified by any of these routes.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The laboratory maintains an active security program where the security of alarmed portions of the laboratory are tested and results recorded. There were no unexplained alarm events and there were no faults in the alarmed systems that were tested. There were no breaches to the laboratory nor to the equipment or databases that it houses. More importantly, there were no electronic data breaches in the laboratory.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The efficacy of the OPD Criminalistics Laboratory DNA analysis program is illustrated by citing the following compelling statistics:

The laboratory completed 430 requests in 2021. These are further broken out by crime type in Table 1 below

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2021

Crime Type	**Number of Requests**
Homicide	92
Attempted Homicide	18
Cold Case Homicide	2
Suspicious Death	1
Rape	114
Other Sexual Assault (not rape)	57
Kidnapping	1
Assault	49
Robbery	29
Burglary	12
Carjacking	9
Hit and run	2
Auto Theft	1
Weapons	35
Other Person	4
Other Criminal	3
Officer Involved Shooting	1
Total	**430**

CODIS hits in 2021 – One hundred and twenty-four DNA profiles were uploaded to the CODIS database. The laboratory had one hundred and seventeen associations (hits); seventy-two hits to named individuals whose identity were unknown, seven hits to unsolved forensic cases, and thirty-eight hits to previously solved forensic cases.

Thus, forensic DNA analysis is an important tool to investigate and provide potential leads for a variety of crimes that occur in the City of Oakland.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no public record requests for DNA analysis.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Procurement of instruments is costly and is typically amortized over many budget cycles. Ongoing maintenance is imperative to ensure reliability of the instruments is remediated quickly should a problem occur. The reagents/kits and supplies to conduct testing are also steep. The cost / benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at $10,000,000 and a return seen of $135[1] per dollar spent on violence reduction. Similarly, economic studies show that investigating sexual assaults results in $81[2] saved per dollar spent.

The total costs of procuring and maintaining the equipment are shown by Category of testing and platform below:

Digestion/Extraction

- *EZ1: $63,000 to purchase (x3 instruments = $189,000) and $3,100 to maintain; 3 instruments for $9,300 annual*
- *Versa 1100: $85,000 to purchase and $6,800 to maintain*

DNA Quantitation

- *Qiagility: $33,100 to purchase (x3 instruments = $99,300) and $2,700 to maintain; 3 instruments for $8,100*
- *QuantStudio 5: $57,000 to purchase (x2 instruments = $114,000) and $5,100 to maintain; 2 instruments for $10,200*

DNA Normalization / Amplification

SpeedVac: $4,000 to purchase, no maintenance
ProFlex Thermalcyclers: $14,000 to purchase (x2 instruments = $28,000), no maintenance

DNA Typing

3500: $135,000 to purchase, $6,000 to maintain

DNA Interpretation

STRmix: $66,000 to upgrade, $22,000 to maintain
FaSTR: $37,000 to purchase, $8,000 to maintain
ArmedExpert: $15,000 to purchase

[1] Abt, Thomas (2019). Bleeding Out: The devastating consequences of urban violence—and a bold new plan for peace in the streets. Chapter 11, p. 208.
[2] Wang and Wein (2018) Journal of Forensic Sciences, Analyzing Approaches to the Backlog of Untested Sexual Assault Kits in the USA, July 2018, Vol. 63, No. 4, pp. 1110-1121.

The cost of testing reagents/kits was approximately $131,000, however, this does not include consumables such as scalpels, masks, gloves, plastics, slides nor serological test kits.

Total purchase cost (born over several years): $772,300
Total maintenance cost, 2021: $70,400
Total testing cost reagents/kits, 2021: $131,000
Estimate of consumables: $140,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

The instruments and software listed in the September 2020 Surveillance Impact Report (SIR) and Biometric Technology Use Policy (SUP) were not replaced during 2021. The laboratory did take some instruments and software out of service and replaced with technology platforms already included in the SIR and SUP (e.g. the Proflex and 3500 instruments).

For the current year, the laboratory is in the process of replacing the three Qiagen EZ1 robots (14 sample capacity) with two EZ2 robots. The EZ2 robot has a larger capacity (24 sample capacity) and will increase the number of samples processed in the same amount of time. The EZ2 robots were purchased with FY2020 Capacity Enhancement and Backlog Reduction (CEBR) grant funds as declared in resolution 88358 for which purchase permission was granted; they are ordered, and the laboratory awaits shipment.

Later this year, when FY2021 CEBR grant funds become available, four cold storage units (freezer/refrigerator and refrigerator) will be replaced as declared in resolution 89011. The laboratory is also in the planning stages for STRmix software validation which has been disclosed in the existing SIR and SUP.

No new biometric capacities were added to the laboratory during 2021.
The laboratory is proposing a few changes to the current SUP and SIR 1) to reflect the technology that has been retired or replaced and 2) to add language codifying current OPD criminalistics laboratory practices which prevent improper use of victim profiles.

Edits in the SUP and SIR address retired or replaced technology.

Codification of Prevention of Improper use of Victim Profiles

In the past, the Forensic Biology unit QC database contained DNA profiles obtained from blood samples associated with homicides, suspicious circumstance deaths, and sexual assault cases. These blood samples were anonymized, assigned a QC source number and used as positive control samples for casework analysis. The purpose of using these QC samples was to show that the testing method or DNA typing process worked by verifying that expected results were obtained. This process was performed from 1996 to 2011. In 2012, the anonymized DNA profiles obtained from these samples was included in the QC database described above for the purpose of quality checks of backlogged or re-sampled

cases. The source of the profiles is unknown to crime lab line staff. They have never been, nor will they ever be, used for the identification of an individual in a criminal matter. Nevertheless, and in an abundance of caution, these QC samples were removed from the active database and archived in a location only accessible by FBU Supervisors. Additionally, language specifying that these profiles cannot be used for associations is proposed to be added to the SUP.

The Forensic Biology unit maintains an in-house Quality Control (QC) database. The QC database contains DNA profiles obtained from the following sources:

1. *By consent from OPD staff (current and past) and their family members. OPD personnel that may enter the chain of custody for an evidence item or has other contact within the scope of the case,*

2. *Samples provided by accredited proficiency test providers. The samples are anonymized by the test provider; the test providers are subject to strict confidentiality requirements by the accrediting bodies. The laboratory has no access to the source of these samples.*

3. *The purpose and use of the QC database is twofold: 1) for casework quality control checks to ensure that the process worked correctly (positive control) and 2) to determine if there is possible contamination from a known individual to a casework sample. At this time, there are no victim references in the QC database. Such profiles have never been, nor are they allowed to be, used for the identification of an individual in a criminal matter.*

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Dr. Sandra Sachs, Criminalistics Laboratory Manager, at ssachs@oaklandca.gov.

Respectfully submitted,

_____

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Prepared by:
Sandra Sachs, PhD, Crime Lab Manager
OPD, Criminalistics Laboratory

Bonnie Cheng, Acting Forensic Biology Unit Supervisor
OPD, Criminalistics Laboratory

Bruce Stoffmacher, Privacy and Legislation Manager
OPD, Bureau of Services

Attachments (1)
A: Criminalistics Laboratory - Requests Completed Between 01 Jan 21 and 31 Dec 21

CITY OF OAKLAND

MEMORANDUM

TO:	LeRonne L. Armstrong, Chief of Police	**FROM:**	Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations
SUBJECT:	Forensic Logic CopLink System – 2021 Annual Report	**DATE:**	March 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Captain Paul Figueroa, Criminal Investigations Division Commander, was the Program Coordinator for 2021.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Forensic Logic search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- *License plate numbers*

- *Persons of interest*
- *Locations*
- *Vehicle descriptions*
- *Incident numbers*
- *Offense descriptions/penal codes*
- *Geographic regions (e.g., Police Beats or Police Areas)*

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud and encryption of data both at rest and in transit is protected by being compliant with FIPS 140-2.

In 2021, there were a total of 573 distinct users who conducted Forensic Logic searches, for a total of 498,267 separate queries. Table 1 below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CopLink Searches; by Distinct User and Search Totals

Search Type	***January***	***February***	***March***	***April***	***May***	***June***
Number of OPD distinct users in each month	*345*	*352*	*345*	*359*	*365*	*366*
Number of searches conducted	*41,665*	*46,601*	*45,940*	*47,718*	*43,929*	*40,302*

Search Type	***July***	***August***	***September***	***October***	***November***	***December***
Number of OPD distinct users in each month	*342*	*336*	*342*	*334*	*313*	*307*
Number of searches conducted	*40,141*	*42,506*	*36,149*	*45,949*	*33,725*	*33,642*

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Data searched with the Forensic Logic CopLink system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other Forensic Logic client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the Forensic Logic cloud repository, it is made available to agencies subscribing to the Forensic Logic service who are permitted by their agency command staff to access CJIS information[1].

[1] Below is the warning message on the service user sign-on page that every user sees prior to accessing the system:

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to.

The CopLink service is accessible by authorized OPD users on OPD computers with appropriate an user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- *Arrest records*
- *Field contacts*
- *Incident reports*
- *Service calls*
- *Shots fired (ShotSpotter)*
- *Stop Data reports*
- *Traffic Accident reports*

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

CopLink software is not deployed in a manner as is physical hardware technology. The software is used by OPD personnel at the Police Administration Building, Eastmont Building, Communications Center, the Emergency Operations Center, (when active) and in patrol vehicles to search crime incidents and related data. The data itself can relate to crime data with geographic connections to anywhere in the City as well as the broader region and even nationally.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each CopLink query. There are thousands of queries and not all queries would provide race data of each suspect or person connected to each data result. Staff therefore recommend that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

Forensic Logic conducted an audit of OPD system queries to ensure all logins were conducted by existing OPD personnel

Forensic Logic is notified of additions or deletions to its subscription services by the designated Point of Contact at the Oakland Police Department. Forensic Logic also would modify the user census upon the request of any Chief of Police, Assistant Chief of Police or Deputy Chief of Police of the Oakland Police Department.

In addition, all Oakland Police Department users can only use Forensic Logic services from within OPD designated facilities such as the Police Administration Building, the Eastmont satellite location, the Communications Center, the Emergency Operations Center and from inside a patrol vehicle due to Forensic Logic's requirement that Internet Protocol (IP) addresses for users be whitelisted (be enabled for access). Any attempt to log in to the Forensic Logic services outside of those locations would fail by any person with an authorized OPD user id (email address).

In addition, on an annual basis, Forensic Logic will prepare a list of enabled OPD users for review by the OPD Point of Contact to confirm that all users should be enabled for access to the Forensic Logic services. Should individuals need to be removed from the services, the Point of Contact will notify Forensic Logic at that time.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

Neither OPD, Oakland Information Technology Department, nor Forensic Logic are aware of any data breaches.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are no existing or newly opened public records requests relating to Forensic Logic, CopLink, or LEAP (former name for CopLink).

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Tables 2 and 3 below provides costing data from the current Oakland Forensic Logic contract.

Table 2: Oakland Forensic Logic Contract Cost; July 2020 - June, 2022

For the Period 07/01/2020 through 06/30/2022 payable upon execution of agreement:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH (07/01/20-06/30/21)	$275	$199	794	$158,006	0%	$158,006
	CopLink Analytics (07/01/20-06/30/21)	$1,000	$1,000	794	$794,000	100%	$0
	CopLink CONNECT (2 Years)	$20,000	$20,000	1	$20,000	0%	$20,000
	Integration Services NIBIN	$5,000	$5,000	1	$5,000	0%	$5,000
	Integration Services Motorola Premiere One CAD and RMS	$25,000	$25,000	1	$25,000	0%	$25,000
	CopLinkX (07/01/21-06/30/22)	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($356)	1	($356)		($356)
						TOTAL	$451,000

Table 3: Oakland Forensic Logic Contract Cost; July 2022 - June, 2023

For the Period 07/01/2022 through 06/30/2023 payable on July 1 2021:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH						
	CopLink Analytics						
	CopLink CONNECT	$10,000	$10,000	1	$10,000	0%	$10,000
	CopLinkX	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($350)	1	($350)		($350)
						TOTAL	$253,000

K. <u>Any requested modifications to the Surveillance Use Policy and a detailed basis for the request</u>:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief of Police
OPD, Bureau of Investigations

Reviewed by,
David Elzey, Captain
OPD, Criminal Investigations Division

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne Armstrong, Chief of Police

FROM: Robert Rosin Acting Captain of Police

SUBJECT: Pursuit Mitigation System – 2021 Annual Report

DATE: February 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-22: Pursuit Mitigation System requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and Public Safety Committee. The information provided below is compliant with the annual report policy requirements of DGO I-22 as well as OMC 9.64.040.

Acting Captain Rosin, Bureau of Field Operations I, Area 2, is currently the Pursuit Mitigation System Coordinator.

DGO I-22 explains that "StarChase," a private company, manufactures and supports its Pursuit Mitigation GPS Tag Tracking System. The "StarChase" system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle.
The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

2021 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

GPS Tag technology was deployed one (1) time in 2021. On New Year's Eve 2021, OPD received information of an armed caravan assembling in a West Oakland neighborhood. Plain clothes officers were dispatched to the area to investigate and make observations from a safe distance. A suspect vehicle from a previous armed caravan incident was observed. The vehicle left the area and separated from the

caravan. OPD personnel attempted a traffic stop, but the suspect vehicle evaded OPD patrol vehicles; no pursuit was initiated or authorized. Later, an OPD officer was able to position the patrol vehicle behind the suspect vehicle. OPD Command approved the deployment of the GPS Tag in order to assist in the safe apprehension of the suspect. One GPS Tag was launched at the rear of the vehicle but failed to affix properly and subsequently fell off the vehicle. There was no active tracking yielded from the GPS Tag deployment.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

No GPS Tag data was generated from this one use.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

n/a

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

The technology was deployed on Interstate 80 near the city of Vallejo, outside of the City of Oakland.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff. The suspect connected to the vehicle where the GPS Tag Tracker was deployed was (one) male African American.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There were no audits as the technology was deployed only once, the use was in alignment with DGO I-22, and no data was generated.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no Pursuit Mitigation System technology data breaches as there was no data generated.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Table 1 below provides 2021 Part 1 Crime Data. The Crime Data report shows the high level of many types of Type 1 violent crimes occurring throughout the City. OPD uses surveillance technology to address this high level of crime.

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no public records requests (open or closed) related to GPS Tag technology in 2021.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

OPD anticipates that the annual cost – once deployed – will be approximately $30,000 annually for unlimited data and mapping service. This expense will be supported from OPD's database subscription account.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

While there was just one deployment of the GPS Tag system in 2021, OPD Command Staff has a plan to re-highlight the importance of the use of the GPS Tag technology as it relates to pursuit mitigation. The Training Section will produce a video which demonstrates the use of the GPS tag system and covers some of the relevant policy points which will help officers remember to request/use the technology during stressful enforcement action when split-second decisions are crucial. Additionally, OPD will move all vehicles equipped with the GPS Tag systems to the Patrol Division. Patrol Officers are engaged with more pursuits than other units because they have fewer resources available to follow and are more often responding to crimes in progress than special duty teams.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments as well as the reporting requirements of OMC 9.64.040. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Robert Rosin, Acting Captain
OPD, Bureau of Field Operations 1, Area 2

Reviewed by,
Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Roland Holmgren, Captain
OPD, Violent Crime Operations Center

Prepared by:
Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Section

CITY OF OAKLAND

MEMORANDUM

TO:	LeRonne Armstrong, Chief of Police	**FROM:**	Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations
SUBJECT:	Mobile Fingerprint ID– 2021 Annual Report	**DATE:**	March 15, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The City Council adopted Resolution 88095 C.M.S. on April 7, 2020 which approved the OPD Mobile ID Surveillance Use Policy as well as the Surveillance Impact Report.

OPD does not currently possess any Mobile Identification Devices (MID)s and there was zero (0) MID usage by OPD in 2021. The Alameda County Sheriff's Office (ACSO), the lead sponsor of the MID program, is currently upgrading the devices with technology provider. OPD will appoint an internal MID Coordinator when OPD is able to receive and deploy upgraded units.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

The Surveillance Impact Report for the Mobile Identification Device MID explains that, "Mobile Identification Devices (MID) are small enough to be handheld, and contains an optical sensor to scan fingerprints and transmit them to look for matches within local databases MIDs are not investigative tools – they only allow personnel to attempt to match fingerprints of individuals who are to be arrested with possible matches from past arrests in Alameda and Contra Costa Counties.

The MID uses the Bluetooth radio standard to send a scanned image of a fingerprint to a police vehicle mobile data terminal (MDT), which can connect with special software. The software accesses a regional fingerprint database shared by Alameda and Contra Costa Sheriff's Offices called Cogent Automated Fingerprint Identification System (CAFIS).

The sole purpose of the MID is to allow police to identify individuals who do not possess acceptable forms of identification (e.g. driver's license or passport) in cases where they otherwise do not need to be booked in the Alameda County Jail. State law requires police to identify individuals to be cited for an infraction or misdemeanor; arrest and booking into jail is legally required when an acceptable form of ID cannot be obtained. Police need to know who you are when a citation is appropriate."

OPD did not possess nor deploy MIDs in 2021.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

There was no usage and no data generated in 2021.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

MIDs are not attached to any fixed objects.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

OPD did not deploy MIDs anywhere in the City in 2021.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There was no usage of MIDs and no data or usage to audit.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There was no MID-related data generated and no data breaches.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Non applicable based on zero usage.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

No public records requests related to MIDs in 2021.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

There was no MID usage and no cost to OPD.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeffrey Thomason, Lieutenant
OPD, Special Operations Section

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne Armstrong, Chief of Police

FROM: Trevelyon Jones, Captain, Ceasefire Section

SUBJECT: Gunshot Location Detection System (ShotSpotter) – 2021 Annual Report

DATE: March 22, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended adoption of OPD Department General Order (DGO) I-20: "Gunshot Location Detection System" at their October 3, 2019 meeting; the report was presented to the City Council on November 19, 2019 and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2021 Data Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the "Surveillance Impact Use Report for the Gunshot Location Detection System:"

Part 1 – How the System Works: "The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g. broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the "ShotSpotter Cloud" determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing

information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average)."

From Section 2: Proposed Purpose: "The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data."

ShotSpotter technology was used in the following ways/with the following outcomes in 2021:

- *The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 8,965 unique gunshot incidents from January 1 – December 31, 2021. Of those alerts, 8,922 (99%) were not called in by the community as a 415GS call type (shots fired), and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 300 feet of a ShotSpotter alert.*
- *ShotSpotter led police to 86 shooting victims when no one called 911, 10 of which were homicides and 76 were injured. OPD was able to provide and coordinate immediate emergency medical response to the 76 surviving shooting victims; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 10 minutes and 1,000 feet of the location where the victim was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 86 cases cited here (76 injury cases) are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.*
- *ShotSpotter activations led OPD to 67 victims where their vehicle and/or dwelling was shot. Of these 67 victims, 28 victims were present but not hit by gunfire, and 39 were listed as victims because the property belonged to them.*
- *1,530 crime incident reports (17% of total activations)*
  - *1,108 (72%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.*
- *ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:*
  - *Seventeen detailed forensic reports*
  - *Court preparation for eight cases*

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The following agencies have been provided log-in access to the ShotSpotter System for ongoing usage:

1. *OPD and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gun shots. This MOU allows OPD to share access to the ShotSpotter cloud-based portal with OHA PD personnel.*
2. *Personnel from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) who participate in the Council-approved OPD-ATF Taskforce also have access to the ShotSpotter System.*

These agencies have ongoing log-in access and do not make written requests for access.

DGO I-20 Section B – 1. "Authorized Use" states:

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel, authorized members of agencies working in contracted partnership with OPD, and members of agencies specifically designated for temporary authorization by the Chief of Police, shall be granted access to OPD's GLD System. The Chief of Police may designate temporary authorization to utilize OPD's GLD system to members of agencies working in partnership with OPD within the City of Oakland.

The California Highway Patrol (CHP) requested ShotSpotter access during the May Day event in 2021 when there were hundreds of people at large events in the downtown area. However, command approval was not granted in time for this request; ultimately, no access was granted.

Separate from ongoing login access, DGO I-20 provides rules for sharing ShotSpotter System data with outside agencies. Section C–3 of DGO I-20: "GUNSHOT LOCATION DETECTION SYSTEM" – "Releasing or Sharing GLD System Data," states:

"GLD system data may be shared only with other law enforcement or prosecutorial agencies based on a need to know or a right to know, or as otherwise required by law, using the following procedures:

1. *The agency makes a written request for the ShotSpotter data that includes:*
    a. *The name of the requesting agency.*
    b. *The name of the individual making the request.*
    c. *The need for obtaining the information.*
2. *The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.*
3. *The approved request is retained on file and shall be included in the annual report.*

OPD did not provide specific ShotSpotter data to outside law enforcement agencies in 2021. However, OPD investigators in the Criminal Investigations Division and or other sections of OPD such as the Ceasefire Section regularly communicate with personnel from other law enforcement agencies on interjurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter

activations. ShotSpotter activations many times may lead to evidence gathering (e.g., finding bullet casings); OPD may share information about evidence (e.g., that bullet casings were found in a particular area at a particular time).

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles or approximately 32 percent of the city land size (55.93). OPD has chosen to install the sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system.

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gun shot, and one second after.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

***Attachment A** to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter "phases" or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all five official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity. **Attachment B** to this report is a weekly public ShotSpotter Activation Report for the week of March 22-28, 2021; this later report highlights areas of Oakland where ShotSpotter alerts have most recently occurred.*

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter and the administrative burden (6,053 total 2021 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided direction that covers login, and how to use different views (e.g., time-period).

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter has verified that for 2021, all users who logged into the system were authorized users.

Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. Shotspotter can only audit logins for both the Respond and the Insight program. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly removes access from employee emails where staff separate from City employment.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

Neither OPD, ShotSpotter, nor the city's IT Department are aware of any data breaches of ShotSpotter data or technology in 2021.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year

Table 1: 2021 OPD Type 1 Crime Data

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• Homicide - all other *	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• With Firearm	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• Auto	6,221	8,179	31%	8,921	-8%
• Residential	1,247	1,055	-15%	1,370	-23%
• Commercial	958	670	-30%	750	-11%
• Other/Unknown	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

Table 2: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2021

Cases by Firearm-Related Crime Type	**No.**
Homicide	27
Attempted Homicides	6
Assault with a Firearm	186
Shoot at an Occupied Home/Vehicle	93
Shoot at an Unoccupied Home/Vehicle	88
Negligent Discharge of a Firearm	1,076
Weapons Violations (including exhibit/draw)	11
Robbery with a Firearm	10
Other (non-firearm crime type)	29
Total Cases	**1,530**

Table 3: Firearm Recoveries in 2021 Connected to ShotSpotter Activations illustrate Guns Recovered

Firearm-Related Crime Type	No.
Homicide	15
Assault with a Firearm	31
Shoot at an Occupied Home/Vehicle	3
Shoot at an Unoccupied Home/Vehicle	1
Negligent Discharge of a Firearm	17
Weapons Violations (including exhibit/draw)	18
Battery	0
Oher (non-firearm related)	3
Total Cases	**88**

- *88 weapons seized.*
  - *Note: more than one firearm may be from the same incident.*
- *700 incidents when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters**,** high capacity or automatic weapons being used, and drive-by shootings.*

Table 4: Cases Where ShotSpotter Notifications Resulted in Gunshot Victim Medical Support

Dispositions	Incidents
Murder	10
Assault Firearm	75
Attempted Murder	1
Total Cases	**86**

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are six existing and/or new (five current) public records requests (PRR) in 2021.

1. *RT – 16562*
2. *RT – 20137*
3. *18-4226*
4. *19-3007*
5. *21-6666*
6. *21-7783*

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Total paid in 2021 was $592,010 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for policy changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Trevelyon Jones, Captain, OPD, Ceasefire Section, at tjones@oaklandca.gov

Respectfully submitted,

Trevelyon Jones

_____

Trevelyon Jones, Captain, OPD, Ceasefire Section

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Paul Figueroa, Captain
OPD, Criminal Investigations Division

Carlo Beckman, Police Services Manager
OPD, Research and Planning Section

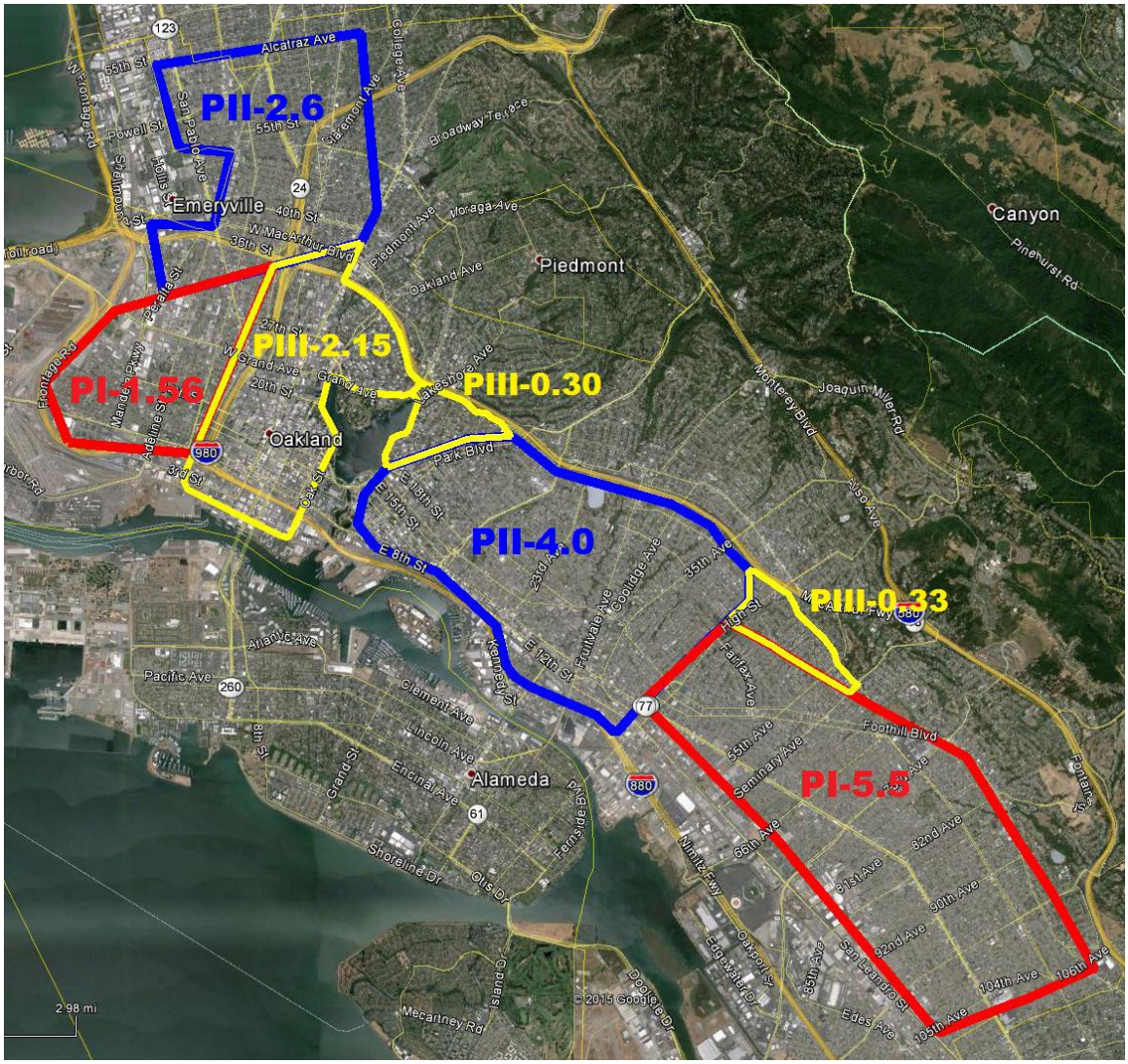
Prepared by:
Bruce Stoffmacher, Privacy and Legislation Manager
OPD, Bureau of Services

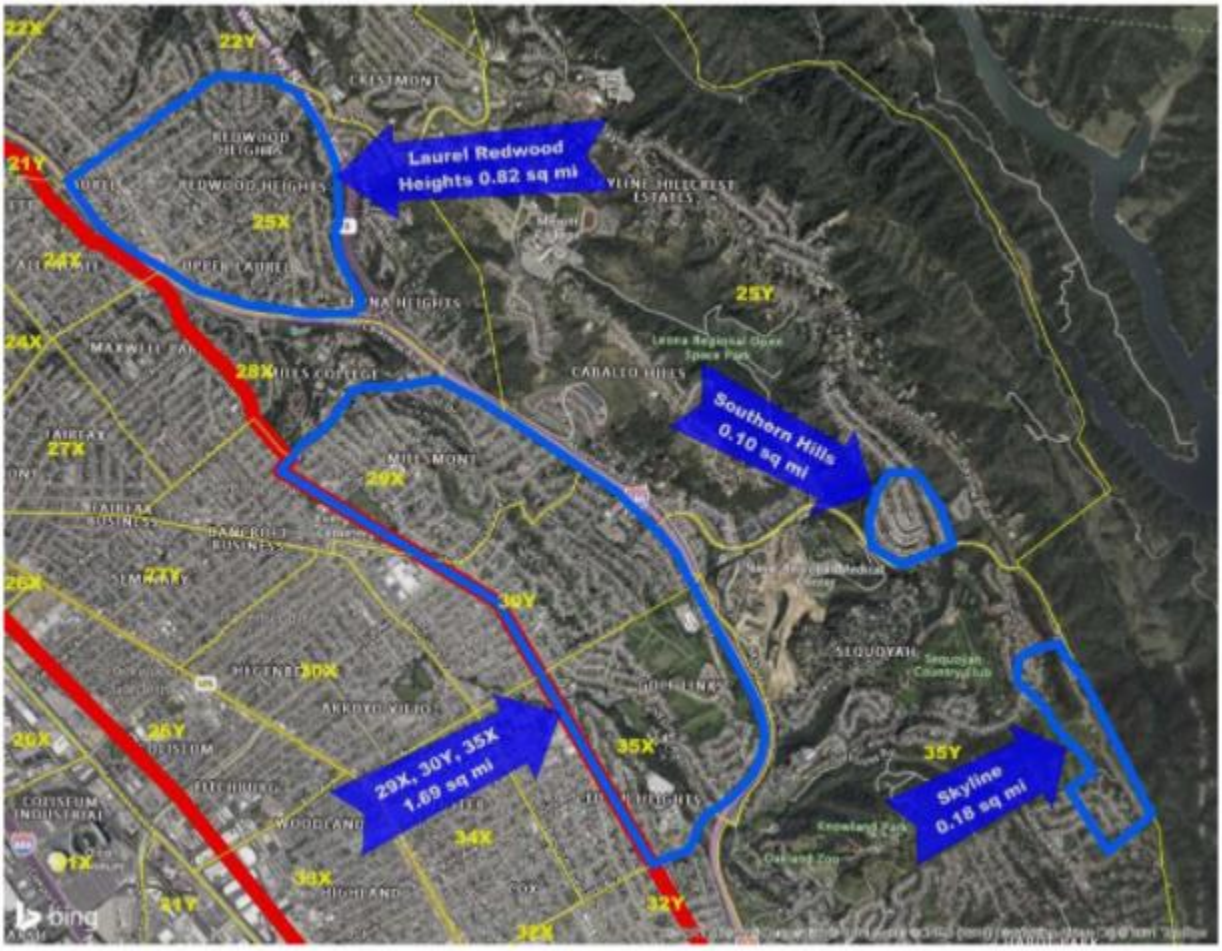
Attachment A - Shot Spotter Coverage Areas

Phase I with red borders (Activated in 2006): 6.2 square miles
East Oakland: East of High Street to 106th Avenue
West Oakland: East of Highway 980 to Frontage Road

Phase II with blue borders (Activated in 2013): 6.4 square miles
East Oakland: West of High Street to Park Boulevard
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles
Downtown Oakland: Jack London Square to about West MacArthur Boulevard
Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard
Maxwell Park: East of High Street to Highway 580 & Mills College




Laurel Redwood Heights 0.82 sq mi
Southern Hills 0.10 sq mi
29X, 30Y, 35X 1.69 sq mi
Skyline 0.18 sq mi
22Y
21Y
25X
24X
24X
28X
25Y
27X
29X
27Y
26X
30Y
30X
26X
26Y
35X
35Y
34X
38X
31Y
32Y
32X
bing

CITY OF OAKLAND

MEMORANDUM

TO:	LeRonne Armstrong, Chief of Police	**FROM:**	Drennon Lindsey, Deputy Chief of Police OPD, Bureau of Investigations
SUBJECT:	Unmanned Aerial System (UAS or Drone) – 2021 Annual Report	**DATE:**	March 9, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC voted unanimously to recommend City Council adoption of OPD's Departmental General Order (DGO) I-25: Unmanned Aerial System (UAS) Use Policy on May 14, 2020. The City Council adopted Resolution No. 88454 C.M.S. which approved OPD's DGO I-25. OMC 9.64.040 requires that, after City Council approval, OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

Lieutenant Daza-Quiroz is currently the UAS Program Coordinator.

2021 Data Points

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the "Surveillance Impact Use Report for the Unmanned Aerial System (UAS)"

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means.

UAS are controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAV its surroundings from a birds-eye

perspective. UAV pilots can leverage control unit applications to pre-program specific GPS coordinates and create an automated flight path for the drone.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS proposed for use by OPD and/or the Alameda County Sheriff's Office use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

UAS technology was used in the following ways/with the following outcomes in 2021:

Fifty-One (52) uses. Currently, OPD has no ownership of UAS's. All deployments and missions are conducted by the Alameda County Sheriff's Office (ACSO) or neighboring agencies with UAS Programs. In 2021, ACSO, and San Leandro Police Department (SLPD) responded to OPD requests. ACSO at times monitors radio channels and will respond prior to being requested[1]. However, all agencies will only deploy if requested by an OPD commander and if policy requirements are met. OPD ESU has created a spreadsheet to track and monitor outside agency deployments. Lt. O. Daza-Quiroz sent a department wide email mandating all commanders who deploy drones to author documentation, similar to the protocol for use of the Emergency Rescue / Armored Vehicles. This process has allowed for appropriate documentation.

Table 1 below details the deployments of ACSO Drones in 2021 in the City of Oakland

Table 1: 2021 ACSO OPD Drone Deployments

Incident Type	***Number***
Mass casualty incidents	*0*
Disaster management	*0*
Missing or lost persons	*3*
Hazardous material releases	*1*
Sideshow events	*4*
Rescue operations	*1*
Training	*0*
Barricaded suspects	*13*
Hostage situations	*0*
Armed suicidal persons	*1*
Arrest of armed and/or dangerous persons	*21*
Scene documentation for evidentiary or investigation value	*7*
Operational pre-planning	*1*
Service of high-risk search and arrest warrants	*0*
Exigent circumstances	*0*
Total	***52***

Additionally, there were six incidents where ACSO responded and did not deploy. Reasons noted for these 'non-deployments were: inclement weather and suspect(s) already detained prior to arrival.

[1] ACSO has access to OPD radio channels and can monitor; ACSO personnel at times can respond to a call for service.

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

(52) Fifty-Two. Outside Law Enforcement Agencies have access to UAS technology, and both provides OPD with the recordings and stores the information in their logs per their respective policy requirements.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The technology was never installed upon fixed objects.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year

Table 2 below details the Police Areas where UAS were deployed in 2021.

Table 2: OPD UAS Deployment by Police Area

Deployment by Area	***Total Deployments***
Area 1	*9*
Area 2	*5*
Area 3	*9*
Area 4	*8*
Area 5	*17*
Citywide	*4**
Total*	***52***

** There were four deployments for Sideshow which were not documented as a specific area; the sideshow activity involved moving vehicles and involved multiple police areas.*

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

Table 3 below provides race data related to 2021 UAS deployments.

Table 3: Race of Detainees Connected to OPD UAS Deployments in 2021

	Race – Female	***Race - Male***	***Total***
Black	*2*	*18*	*20*
Hispanic	*0*	*5*	*5*
Asian	*2*	*1*	*3*
White	*1*	*1*	*2*
Other	*0*	*1*	*1*
Total			***31***

OPD knows the race of detainees connected to UAS deployments. However, the race of individuals involved in many UAS deployments is not known. There are cases such as barricaded suspects, where no suspect is ever discovered or detained. There could also be UAS uses for missing persons where the person's identity is not entirely known nor discovered.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information

The OPD Electronic Surveillance Unit (ESU) maintained a list of all UAS deployment logs for record and tracking purposes. This list was reviewed periodically for accuracy and for assessment of any policy violations. All OPD commanders were directed to send communications to ESU for any UAS request or use – similar to OPD protocols for use of Emergency Rescue / Armored Vehicles. No policy violations were found, and no corrective actions were warranted nor needed in 2021.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

OPD is not aware of any data breaches; ACSO has confirmed that they have not discovered any data breaches

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 4 below provides 2021 Part 1 Crime Data. This data illustrates the high levels of both violent crime and property crimes that occur in Oakland including for the 2021 year. UAS deployments connect to this citywide data in several ways. For example, barricaded suspect incidents are related to several types of crimes listed below. Similarly, arrest of

armed and dangerous suspects, and crime scene documentation also relate to this citywide crime data.

Table 4: 2021 OPD Type 1 Crime Data

Part 1 Crimes *All totals include attempts except homicides*	**01-01-2020 through 12-31-2020**	**01-01-2021 through 12-31-2021**	**Year-to-Date % Change 2020 vs. 2021**	**3-Year Year-to-Date Average**	**YTD 2021 vs. 3-Year YTD Average**
Homicide - 187(a)	102	124	22%	100	24%
• **Homicide - all other ***	7	10	43%	7	50%
Aggravated Assault	3,315	3,559	7%	3,206	11%
• **With Firearm**	499	599	20%	462	30%
Rape	217	158	-27%	193	-18%
Robbery	2,417	2,693	11%	2,641	2%
Burglary Total	8,689	10,197	17%	11,291	-10%
• **Auto**	6,221	8,179	31%	8,921	-8%
• **Residential**	1,247	1,055	-15%	1,370	-23%
• **Commercial**	958	670	-30%	750	-11%
• **Other/Unknown**	263	293	11%	249	18%
Motor Vehicle Theft	8,722	9,010	3%	8,071	12%
Larceny	5,974	6,186	4%	6,643	-7%
Arson	193	170	-12%	172	-1%
Total Part 1 Crimes	29,636	32,107	8%	32,324	-1%

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates.

There were two public records requests (PRR) opened in 2020 that have not been closed as of December 31, 2021, relating to drones:

- *20-3056; and*
- *20-6466.*

OPD's Records Division is still processing these two PRRs in 2021 and into 2022 because the full information request in each case is very broad and extends beyond the one technology or specific uses.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year

($0.00) Zero. OPD did not incur any maintenance, licensing, or training costs.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

No requests for policy changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeff Thomason, Lieutenant
OPD, Support Operations Section

Prepared by:
Omar Daza Quiroz, Lieutenant
OPD, Electronic Support Unit (ESU)

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

CITY OF OAKLAND

MEMORANDUM

TO: LeRonne Armstrong, Chief of Police

FROM: Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations

SUBJECT: Live stream transmitter– 2021 Annual Report

DATE: March 15, 2022

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) I-23: Live Stream Transmitter Use Policy governs OPD's use of Live Stream Transmitters; the policy was approved by the City Council on April 21, 2020 through Resolution No. 88099 C.M.S., as well as OMC 9.64.040, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council. The information provided below is compliant with the annual report policy requirements of OMC 9.64.040 and DGO I-23.

Sergeant Inez Ramirez is currently the Live Stream / Video Team Program Coordinator.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

OPD used the livestream transmitter technology one time in 2021. ***Attachment A*** *to this report provides the detail from the required after-action report provided to the City's Privacy Advisory Commission (PAC) as well as the City's Chief Privacy Officer. From page one of the report:*

"The City of Oakland activated its Emergency Operations Center (EOC) on May 1, 2021 and, as part of the City's Incident Command System response, OPD staffed the EOC positions therein including the role of OPD Operations Incident Command. The activation and associated operations were necessitated by the plan to address planned but unpermitted crowd management events associated to "May Day" parades, marches, rallies, demonstrations, protests and May 1st events. Although OPD deployed video teams with EOC video stream transmitters during the entire operational period, the technology use was

limited to evening and late evening hours to better assess, plan, direct, and respond to circumstances associated with a march of approximately 70 persons."

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

DGO I-11 does provide that OPD may share live stream data with other law enforcement agencies that have a right to know and a need to know[1], such as an inspector with the District Attorney's Office. However, no live stream data was downloaded, retained, or shared with different agencies. Video was streamed into the EOC/DOC. Any supporting agency inside the EOC would have viewed the live stream. No live stream video was saved/downloaded at the EOC/DOC. No live stream video was shared with other law enforcement agency, unless they viewed it live on the screen at the EOC/DOC. No one is allowed at the EOC without:

1. *Authorization*
2. *Verification of their status, department, rank, and title*
3. *All verifications are documented by OPD and or City Administration.*

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The transmitters are attached to video cameras which are handheld by officers monitoring the events.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

The live stream transmitters were deployed in areas where the protests and marches occurred in parts of downtown Oakland.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

[1] DGO I-23 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.
OPD did notify the City's Chief Privacy Officer and Chair and Co-Chair of the Privacy Advisory Commission on May 3, 2021 of the use of the equipment on May 1, 2021. The report was discussed at the public May 5, 2021 PAC meeting.

In terms of an "analysis shall also identify the race of each person that was subject to the technology's use:"

- *data was not generated from use of the livestream transmitter as the transmission was not recorded; there is no data to analyze.*
- *Additionally, the technology is used to survey a large area for situational awareness. The administration burden would be high and challenging to determine the race of everyone who may have been streamed via the live video during even one usage over the course of an hour or more in an event with hundreds of people.*

For the reasons cited above, staff recommends that the PAC waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by both the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The one use in 2021 was reviewed for adherence to policy and internal protocols:

- *Video was not recorded during the incident (see **Attachment A** for full report);*
- *Appropriate staff were notified of use and the City's Privacy Officer and PAC were notified according to policy.*
- *Technology was properly stored with the OPD Information Technology Unit (ITU).*
- *OPD is not aware of any policy violations from use of the live stream transmitters in 2021.*

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

OPD is not aware of any data breaches; furthermore, data was not generated from use of the livestream transmitter as the transmission was not recorded.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

*The "Report on Video Stream Request and Usage," dated May 3, 201 (**see Attachment A**) explains that the decision to activate live stream and recording during the evening hours:*

- *Video Team assignments and equipment are a recommended if not required component of OPD response to planned events involving potentially large crowds.*
- *Live stream may be authorized by the Incident Commander.*
- *The march was reportedly organized or promoted by the same source linked to a April 16, 2021march that resulted in numerous instances of property damage, arson, assault, and battery of police officers; the apparent organizers or participants of that event had refused to communicate with or otherwise cooperate with police*
- *The imagery used to promote the unpermitted march displayed burning structures with proximate protest activity inferring desired crimes of arson.*
- *The text used in this event's main social media/internet posting urged absences of livestreaming, picture taking, and "snitching" for an inferred intent to commit criminal acts with reduced chances of being identified and arrested.*
- *The text used in this event's main social media/internet posting was inherently anti-police and requested participants to "bring soup." Soup cans were thrown at officers with intent to injure during past anti-police demonstrations including the previously referenced 16 Apr 21 event.*
- *Open media sources had reported "antifa" communication and meetings in nearby Northern Ca communities identifying "May Day" as an opportunity to "kill cops." Persons affiliated with the "antifa" group(s) had ties to past Oakland events in which violence was used.*
- *The social media/internet posting urged persons to wear all black. "Black Blok" is a tactic in which persons desiring to commit unlawful acts wear black clothing so that they may not be easily identified or found within the crowd during or after committing criminal acts.*
- *The vast majority of persons assembled at Frank Ogawa Plaza arrived wearing all black.*
- *Many persons arriving at Frank Ogawa Plaza possessed bulky backpacks. Backpacks have been used to secret "tools of violence" and other instruments to damage property, commit acts of arson, or batter police officers.*
- *Officers observed a bag of canned soup brought to or possessed by persons assembling at Frank Ogawa Plaza.*
- *Attempts to communicate with the persons assembled in Frank Ogawa Plaza failed to achieve cooperation in establishing a march route, police liaison, and means by which criminal activity could be mitigated or otherwise cooperatively addressed.*
- *When persons assembled at Frank Ogawa Plaza entered the roadway with apparent intent to march, I authorized live stream and recording in order to better observe, plan, direct, and assess the crowd control incident in best effort to prevent, record, and address instances of property damage, arson, crime, and assaultive behavior.*

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were no PRRs related to live stream transmitters in 2021.

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

One hundred thirty thousand dollars ($130,000) in one-time purchase cost. In 2021, OPD upgraded the video streaming system that was originally purchased in 2011. This included camera equipment, transmitters, receivers and software licensing.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

Reviewed by,
Jeffrey Thomason, Lieutenant
OPD, Special Operations Section

Prepared by:
David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

Bruce Stoffmacher, Legislation and Privacy Manager
OPD, Research and Planning Unit

Attachments (1)
Appendix A: 2020 Video Stream Deployment Memos

C I T Y O F O A K L A N D

Memorandum

TO: Privacy Advisory Commission and Chief Privacy Officer
FROM: Christopher Bolton, Deputy Chief of Police
DATE: May 3, 2021
RE: Report on Video Stream Request and Usage

This Memorandum summarizes the use of live-stream transmitters by the Oakland Police Department (OPD) in support of the specified event. This memorandum is provided in accordance with OPD Department General Order I-23: "Handheld Livestream Transmitter[1]."

Purpose (from DGO I-23)

Live stream camera transmitters allow OPD to deploy a minimal level of police presence while providing critical situational awareness to OPD commanders. A small number of officers can monitor events and provide real-time footage to Command. This information helps OPD Command to make efficient deployment decisions.

OPD commanders need real time situational awareness to ensure public safety in public spaces. Real-time information regarding events (e.g., crowd management facilitation, coordinated response to catastrophic unplanned events) provides critical information for OPD commanders when making resource deployment decisions. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD without the need to deploy many officers.

Livestream Transmitter Use

The City of Oakland activated its Emergency Operations Center (EOC) on May 1, 2021 and, as part of the City's Incident Command System response, OPD staffed the EOC positions therein including the role of OPD Operations Incident Command. The activation and associated operations were necessitated by the plan to address planned but unpermitted crowd management events associated to "May Day" parades, marches, rallies, demonstrations, protests and May 1st events. Although OPD deployed video teams with EOC video stream transmitters during the entire operational period, the technology use was limited to evening and late evening hours to better assess, plan, direct, and respond to circumstances associated with a march of approximately 70 persons. As the

[1] DGO I-23: Sec. III.B "Restricted Use," Sec 4.ii: ii. For each use of live stream transmitters, OPD shall articulate the facts and circumstances surrounding the use in a written statement filed with the Chief Privacy Officer and/or Chair of the Privacy Advisory Commission within 72 hours. This statement (and the use itself) shall be included in the required Annual Report.

Incident Commander, my decision to utilize video teams with streaming and recording[2] capabilities was based on numerous factors but driven by an overriding desire and mandate to videotape in a manner that minimizes interference with people lawfully participating in First Amendment activities. As evidence of this commitment, video stream was not utilized to record or display the actions of more than 150 persons during the peaceful car caravan and march early within the day. The below is a non-inclusive list of factors informing my decision to activate live stream and recording during the evening hours:

- Video Team assignments and equipment are a recommended if not required component of OPD response to planned events involving potentially large crowds.
- Live stream may be authorized by the Incident Commander.
- The march was reportedly organized or promoted by the same source linked to a April 16, 2021march that resulted in numerous instances of property damage, arson, assault, and battery of police officers; the apparent organizers or participants of that event had refused to communicate with or otherwise cooperate with police/
- The imagery used to promote the unpermitted march displayed burning structures with proximate protest activity inferring desired crimes of arson.
- The text used in this event's main social media/internet posting urged absences of livestreaming, picture taking, and "snitching" for an inferred intent to commit criminal acts with reduced chances of being identified and arrested.
- The text used in this event's main social media/internet posting was inherently anti-police and requested participants to "bring soup." Soup cans were thrown at officers with intent to injure during past anti-police demonstrations including the previously referenced 16 Apr 21 event.
- Open media sources had reported "antifa" communication and meetings in nearby Northern Ca communities identifying "May Day" as an opportunity to "kill cops." Persons affiliated with the "antifa" group(s) had ties to past Oakland events in which violence was used.
- The social media/internet posting urged persons to wear all black. "Black Blok" is a tactic in which persons desiring to commit unlawful acts wear black clothing so that they may not be easily identified or found within the crowd during or after committing criminal acts.
- The vast majority of persons assembled at Frank Ogawa Plaza arrived wearing all black.
- Many persons arriving at Frank Ogawa Plaza possessed bulky backpacks. Backpacks have been used to secret "tools of violence" and other instruments to damage property, commit acts of arson, or batter police officers.

[2] In accordance with DGO I-23, IV.B Livestream Camera Data, "Retention,": Handheld live stream cameras can send the digital stream wirelessly. The EOC does not record this data; data recorded by the handheld cameras is maintained by the OPD IT Unit within in the Bureau of Services (BOS). Personnel using live-stream cameras shall return them at the end of their shift to the IT Unit. For data that is captured and used as evidence, such data shall be turned in and stored as evidence pursuant to existing policy. Otherwise, camera data will be destroyed after 30 days.

- Officers observed a bag of canned soup brought to or possessed by persons assembling at Frank Ogawa Plaza.
- Attempts to communicate with the persons assembled in Frank Ogawa Plaza failed to achieve cooperation in establishing a march route, police liaison, and means by which criminal activity could be mitigated or otherwise cooperatively addressed.
- When persons assembled at Frank Ogawa Plaza entered the roadway with apparent intent to march, I authorized live stream and recording in order to better observe, plan, direct, and assess the crowd control incident in best effort to prevent, record, and address instances of property damage, arson, crime, and assaultive behavior.

RD# or Incident #: 21- 019659
Date of Incident: 1 May 21
Type of Event: Protest
Was EOC/DOC activated: YES
Number of Video Streams provide to EOC/DOC: 3 video streams.
Initial Request: Video Teams were requested by D.C. C. Bolton on 28 Apr 21.

Summary: On 1 May 21 at 2045 hrs. at the direction of D.C. C. Bolton, three video streams were provided by the Video Team to the EOC. The livestream ended at approximately 2230 hrs, when the demonstration ended.

Ann Pierce
Sergeant of Police
Bureau of Investigations
Oakland Police Department

Bruce Stoffmacher
Legislation and Privacy Manager
Research and Planning Section
Oakland Police Department

Oakland Police Department

Criminalistics Laboratory

Requests Completed Between 01 Jan 21 and 31 Dec 21

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
01036278	17022	Sex Offense	1	EK	09/15/20	03/29/21	05/13/21	
01063412	17023	Sex Offense	1	EK	09/15/20	03/29/21	05/20/21	
02001819	17024	Rape	1	EK	09/16/20	03/29/21	05/20/21	
02043259	17025	Rape	1	EK	09/16/20	03/30/21	05/19/21	
02050483	17026	Rape	1	HW	09/16/20	03/30/21	05/20/21	
07026094	5128	Homicide	6	BC	12/08/20	12/09/20	01/14/21	
10023028	6974	Rape	3	CAG	10/14/21	10/22/21	12/30/21	
16031898	10693	Homicide	2	RJ	02/11/21	03/31/21	05/17/21	
16064685	11244	Homicide	4	CAG	04/21/21	04/21/21	05/07/21	
18023529	14166	SC Unexplained Death	3	AL	05/31/18	02/11/21	03/19/21	
18027499	12784	Rape	2	CAG	12/14/20	12/29/20	03/01/21	
18027646	17020	Robbery	2	EK	07/19/18	03/31/21	05/20/21	
18031763	12852	Assault	4	EK	06/28/18	03/31/21	05/20/21	
18033728	17021	Assault	2	NYN	07/11/18	04/01/21	05/20/21	
			3	NYN	08/03/18	04/01/21	05/20/21	
18038487	14949	Weapons	2	EK	08/09/18	03/31/21	05/19/21	
18042053	17058	Carjacking	1	RJ	10/11/18	03/31/21	05/24/21	
18043786	17059	Weapons	2	RJ	08/31/18	03/31/21	06/01/21	
18044586	15313	Robbery	2	SF	09/07/18	06/03/20	10/06/21	
18046211	17060	Other Criminal	4	SF	09/14/18	03/31/21	07/19/21	
18053409	13246	Assault	2	EK	03/07/19	03/31/21	04/29/21	
18055776	13318	Rape	3	HW	04/21/21	04/30/21	05/19/21	
18057757	13520	Homicide	16	HW	12/14/20	01/04/21	01/19/21	
18058849	17061	Robbery	2	SF	11/26/18	03/31/21	07/16/21	
18059648	13383	Homicide	5	RJ	12/06/18	10/29/20	01/29/21	
			7	RJ	12/10/18	10/29/20	01/29/21	
18059725	15124	Robbery	3	HW	11/29/18	02/22/21	05/19/21	
18060226	13421	Weapons	2	RJ	12/18/18	03/31/21	05/11/21	
19000506	13844	Assault	3	EK	07/29/19	05/21/21	10/13/21	
19002000	13664	Robbery	2	VSS	02/14/19	11/24/20	02/02/21	
19003036	17770	Weapons	2	AL	01/25/19	07/28/21	10/11/21	
19003137	13656	Rape	2	HW	01/15/21	01/19/21	02/10/21	
19006349	13634	Assault	3	SF	04/02/21	06/28/21	09/22/21	
19008265	17103	Assault	3	EK	02/25/19	04/05/21	04/29/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
19010466	13706	Assault	2	SF	03/12/19	06/28/21	09/21/21	
19012016	17438	Robbery	4	NYN	03/14/19	05/21/21	08/06/21	
19016757	17340	Weapons	2	AL	04/05/19	05/06/21	06/15/21	
19019197	18017	Robbery	1	VSS	01/21/20	07/13/21	11/19/21	
19022636	14058	Weapons	1	RJ	05/07/19	03/31/21	05/18/21	
19023505	13988	Assault	3	EK	05/15/19	03/30/21	04/29/21	
19028136	17062	Weapons	3	EK	06/07/19	03/31/21	05/11/21	
19029659	17339	Robbery	2	AL	07/08/19	05/06/21	06/15/21	
19030801	17119	Weapons	4	EK	06/20/19	04/06/21	04/29/21	
19034391	14163	Assault	5	EK	07/09/19	03/30/21	04/29/21	
19037014	17846	Robbery	1	SF	07/31/19	08/10/21	10/18/21	
19038175	14227	Assault	3	EK	07/30/19	04/01/21	05/11/21	
19038270	17342	Carjacking	3	EK	07/30/19	05/12/21	06/14/21	
19039295	14221	Assault	2	CAG	08/08/19	04/29/21	07/29/21	
19040045	14953	Homicide	6	HW	02/03/21	02/03/21	04/05/21	
19042455	17290	Burglary	1	CAG	08/26/19	04/30/21	08/11/21	
19042647	16239	Weapons	2	CAG	08/20/19	10/21/20	01/11/21	
19043099	17094	Burglary	2	NYN	08/29/19	04/02/21	05/03/21	
19054375	14447	Robbery	3	EK	03/18/21	08/10/21	11/01/21	
19054399	17343	Sex Offense	1	EK	09/30/19	05/10/21	05/26/21	
19055593	17847	Weapons	1	EK	03/17/21	08/10/21	11/01/21	
19057039	16421	Burglary	1	RJ	11/05/19	11/24/20	01/15/21	
19057574	14479	Assault	2	VSS	11/08/19	03/12/21	04/15/21	
19058068	14485	Assault	1	VSS	11/07/19	03/12/21	04/15/21	
19058600	14504	Homicide	8	CAG	11/19/19	07/23/21	08/11/21	
19058976	15984	Homicide	3	CAG	11/14/19	03/15/21	05/12/21	
19059950	15985	Auto Theft	3	AL	11/21/19	06/07/21	07/09/21	
19060095	14541	Assault	3	AL	04/21/20	06/14/21	07/21/21	
19061640	16420	Robbery	1	VSS	11/26/19	11/24/20	02/08/21	
19062872	16619	Assault	1	AL	12/05/19	12/28/20	02/02/21	
19062955	15400	Weapons	2	SF	12/26/19	04/28/21	07/26/21	
19064132	17848	Robbery	2	HW	12/13/19	08/10/21	10/08/21	
19065714	14686	Rape	2	HW	01/27/21	02/04/21	03/17/21	
19065941	16896	Weapons	1	SF	12/23/19	03/01/21	05/20/21	
19066709	14997	Homicide	2	BC	09/29/21	10/06/21	12/08/21	
19067532	16897	Burglary	1	HW	01/21/20	02/24/21	04/26/21	
20000169	17631	Burglary	1	EK	01/21/20	07/06/21	08/10/21	
20000444	16354	Weapons	4	SF	03/10/21	07/07/21	10/07/21	
20000448	17070	Weapons	1	NYN	01/15/20	03/31/21	05/03/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20000449	17148	Weapons	1	NYN	01/15/20	04/09/21	05/11/21	
20000555	17632	Burglary	1	SF	01/15/20	07/07/21	10/04/21	
20001193	17633	Robbery	1	SF	01/21/20	07/07/21	09/13/21	
20002337	17808	Robbery	1	AL	01/14/20	08/26/21	10/11/21	
20002670	14720	Assault	2	AL	01/16/20	08/26/21	10/11/21	
20003256	17856	Burglary	1	SF	01/27/20	08/06/21	10/11/21	
20003406	14910	Hit and Run	2	VSS	04/13/21	04/20/21	05/17/21	
20003526	17849	Assault	3	EK	01/22/20	08/10/21	10/08/21	
20005624	17920	Burglary	1	EK	02/20/20	08/19/21	10/15/21	
20005838	15204	Rape	3	HW	12/23/20	02/18/21	03/10/21	
20010157	15327	Rape	3	AL	10/13/20	10/19/20	01/14/21	
20011135	17921	Assault	2	SF	03/06/20	08/18/21	12/03/21	
20011754	17079	Robbery	1	EK	08/17/20	04/01/21	04/29/21	
20012506	14850	Weapons	3	EK	03/30/20	04/01/21	04/29/21	
20013312	16355	Robbery	1	RJ	04/15/20	11/10/20	02/19/21	
20014597	17086	Assault	1	EK	03/26/20	04/05/21	05/13/21	
20014820	17380	Homicide	1	AL	05/10/21	05/24/21	07/13/21	
20016868	15010	Weapons	2	SF	03/31/20	05/19/21	07/26/21	
20018666	15160	Assault	1	NYN	04/17/20	05/26/21	08/12/21	
20019001	15279	Homicide	3	SF	04/28/20	08/31/20	04/22/21	
20019026	15926	Robbery	1	SF	04/15/20	08/31/20	03/24/21	
20019050	16512	Weapons	2	HW	04/30/20	12/11/20	01/04/21	
20019088	15110	Assault	3	AL	04/16/20	03/24/21	05/27/21	
20019684	15478	Rape	2	HW	06/16/20	10/27/20	01/04/21	
20019806	16683	Weapons	2	HW	01/19/21	02/16/21	03/19/21	
20020312	15139	Homicide	3	CAG	04/24/20	09/01/21	12/06/21	
20020603	15229	Weapons	2	NYN	05/11/20	05/26/21	07/26/21	
20020660	15140	Weapons	2	SF	04/24/20	09/08/21	11/18/21	
20021531	15173	Assault	3	NYN	04/30/20	03/30/21	05/14/21	
20022305	15332	Sex Offense	2	CAG	05/28/20	11/09/20	03/03/21	
20022757	16881	Carjacking	2	CAG	05/26/20	06/09/21	09/23/21	
20023314	16401	Carjacking	2	VSS	09/23/20	11/19/20	02/19/21	
20025235	17344	Weapons	1	EK	05/26/20	05/10/21	06/14/21	
20025284	15927	Burglary	3	SF	10/19/20	12/07/20	02/09/21	
20026062	17056	Robbery	1	NYN	05/28/20	03/31/21	05/20/21	
20026824	15672	Homicide	3	HW	07/27/20	11/23/20	01/26/21	
20028070	16228	Rape	1	RJ	10/14/20	10/19/20	01/24/21	
20029650	15441	Homicide	3	SF	07/06/20	06/28/21	09/08/21	
20029732	15414	Other Person	1	VSS	06/22/20	07/03/20	02/16/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20030227	15803	Rape	1	SF	08/04/20	08/11/20	05/21/21	
20031564	17012	Carjacking	1	VSS	07/22/20	03/25/21	05/13/21	
20033467	16423	Robbery	2	VSS	07/09/20	11/24/20	02/11/21	
20034591	17418	Assault	3	SF	07/16/20	05/18/21	07/23/21	
20035047	15922	Homicide	3	HW	12/07/20	02/16/21	03/19/21	
20035129	17533	Robbery	2	AL	07/22/20	06/14/21	09/02/21	
20035334	15665	Assault	4	HW	07/21/20	09/17/20	01/06/21	
20035880	15859	Sex Offense	2	HW	07/23/20	10/27/20	01/15/21	
20036082	17527	Weapons	2	CAG	07/24/20	06/09/21	09/20/21	
20037924	16164	Homicide	1	AL	08/05/20	10/05/20	01/20/21	
20038059	17439	Assault	2	CAG	08/04/20	05/24/21	08/19/21	
20038267	15801	Sex Offense	1	VSS	08/05/20	08/11/20	01/15/21	
20038278	15856	Sex Offense	3	HW	01/25/21	01/27/21	03/17/21	
20038696	15879	Attempted Murder	3	AL	11/12/21	12/13/21	12/17/21	
20038766	16403	Attempted Murder	1	HW	10/19/20	11/23/20	01/25/21	
20039000	16296	Robbery	1	RJ	09/03/20	10/29/20	01/04/21	
20039247	15855	Rape	1	SF	08/10/20	08/17/20	01/06/21	
20039558	16231	Rape	1	AL	10/14/20	10/19/20	01/08/21	
			2	HW	10/14/20	11/24/20	01/29/21	
20040117	16425	Assault	1	CAG	08/24/20	11/24/20	03/04/21	
20040194	15972	Rape	1	VSS	09/01/20	09/10/20	05/14/21	
20040600	15920	Weapons	3	SF	09/14/20	12/07/20	04/13/21	
20041076	16404	Rape	1	HW	11/19/20	11/24/20	03/10/21	
20041152	16269	Rape	1	CAG	10/16/20	10/28/20	04/02/21	
20041255	15907	Weapons	2	RJ	08/24/20	03/23/21	06/30/21	
20041382	16298	Sex Offense	1	RJ	10/27/20	10/29/20	02/11/21	
20041824	16165	Assault	1	CAG	09/15/20	10/05/20	01/28/21	
20042634	15993	Rape	1	SF	09/03/20	09/15/20	01/15/21	
			2	SF	07/15/21	07/22/21	10/08/21	
20043707	15967	Attempted Murder	2	SF	09/10/20	12/07/20	03/24/21	
20043942	15995	Rape	1	SF	09/08/20	09/15/20	03/19/21	
20043956	15983	Assault	2	CAG	09/08/20	11/12/20	01/22/21	
20044529	16144	Rape	1	CAG	09/29/20	10/05/20	01/06/21	
20044704	16229	Assault	1	AL	10/14/20	10/19/20	01/08/21	
20045598	17345	Weapons	3	AL	12/10/20	06/15/21	07/27/21	
20045789	16074	Assault	3	HW	09/24/20	11/24/20	02/22/21	
20046588	16153	Rape	1	AL	09/25/20	10/12/20	01/08/21	
20046726	16230	Rape	1	AL	10/14/20	10/19/20	01/20/21	
20047237	16154	Rape	1	HW	09/30/20	10/12/20	01/15/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20047624	16126	Robbery	2	HW	10/19/20	10/27/20	01/06/21	
20047706	16388	Homicide	3	VSS	10/21/20	11/17/20	02/08/21	
20047859	16299	Rape	1	CAG	10/27/20	10/29/20	01/06/21	
20047977	16271	Rape	1	HW	10/21/20	10/28/20	02/08/21	
20048007	16272	Homicide	4	SF	09/01/21	09/27/21	12/13/21	
20048034	16405	Attempted Murder	1	HW	09/22/20	11/24/20	01/29/21	
20048227	16241	Homicide	3	RJ	10/19/20	11/17/20	02/08/21	
20048319	16204	Homicide	1	VSS	10/05/20	10/13/20	02/09/21	
20048495	16422	Assault	1	CAG	10/02/20	11/24/20	02/10/21	
20048886	16291	Assault	2	CAG	10/15/20	11/10/20	01/22/21	
20048907	16202	Homicide	4	VSS	10/26/20	01/15/21	01/27/21	
			6	VSS	11/23/20	12/17/20	01/19/21	
20049373	17742	Homicide	2	AL	10/13/20	07/26/21	10/01/21	
20049517	16337	Rape	1	SF	11/04/20	11/09/20	01/06/21	
20049588	16301	Rape	1	CAG	10/27/20	10/29/20	03/29/21	
20049971	16365	Assault	1	RJ	11/03/20	11/12/20	03/19/21	
20050051	16275	Rape	1	HW	10/14/20	10/28/20	01/04/21	
			2	HW	10/14/20	11/24/20	01/04/21	
20050187	16302	Other Person	1	RJ	10/27/20	10/29/20	01/15/21	
			2	RJ	06/09/21	06/09/21	07/16/21	
20050314	16276	Rape	1	HW	10/21/20	10/28/20	01/08/21	
20050759	16419	Homicide	1	RJ	10/29/20	11/24/20	02/08/21	
20050946	16338	Rape	1	RJ	11/05/20	11/09/20	01/29/21	
20050969	16294	Homicide	3	HW	10/21/20	12/09/20	02/26/21	
			6	HW	11/16/20	08/11/21	10/08/21	
			7	HW	01/04/21	01/05/21	02/26/21	
20051169	16432	Assault	4	NYN	11/12/20	06/18/21	08/12/21	
20051358	16250	Assault	2	CAG	10/21/20	11/24/20	03/04/21	
20051397	16554	Homicide	2	SF	11/16/20	12/15/20	02/11/21	
20051805	16321	Assault	3	CAG	11/16/20	02/04/21	03/24/21	
20051860	16681	Sex Offense	1	RJ	01/05/21	01/08/21	03/01/21	
			2	HW	01/05/21	02/18/21	03/29/21	
20052507	16406	Homicide	3	HW	11/03/20	11/24/20	02/08/21	
20052551	16326	Assault	2	CAG	11/02/20	12/07/20	03/01/21	
20052825	16627	Homicide	1	HW	12/28/20	01/05/21	02/10/21	
20052863	16339	Rape	1	SF	10/28/20	11/09/20	01/06/21	
			2	CAG	10/28/20	01/19/21	05/11/21	
20052901	16409	Homicide	2	VSS	10/29/20	11/20/20	01/25/21	
20053306	16581	Rape	1	CAG	12/09/20	12/21/20	03/22/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20053392	17011	Robbery	3	VSS	11/09/20	03/25/21	05/07/21	
20053459	16398	Rape	1	RJ	11/12/20	11/18/20	01/29/21	
20053480	16767	Homicide	2	CAG	11/19/20	02/01/21	04/19/21	
20053606	16659	Rape	1	RJ	12/23/20	01/08/21	03/01/21	
20053624	16370	Homicide	3	NYN	02/24/21	03/31/21	05/14/21	
20053646	16596	Sex Offense	1	CAG	12/09/20	12/23/20	03/26/21	
20053666	16340	Sex Offense	1	SF	11/05/20	11/09/20	01/06/21	
			2	CAG	11/05/20	01/19/21	05/11/21	
20054210	17010	Homicide	2	AL	11/18/20	03/25/21	05/21/21	
20054745	16693	Homicide	4	HW	01/06/21	02/16/21	02/25/21	
20054927	16625	Sex Offense	1	AL	12/04/20	01/27/21	03/19/21	
20055028	18264	Homicide	1	CAG	11/16/20	10/19/21	12/15/21	
20055058	16399	Rape	2	RJ	11/12/20	11/19/20	01/14/21	
20055306	17923	Homicide	2	EK	03/19/21	08/18/21	10/15/21	
20055519	16395	Attempted Murder	2	HW	11/12/20	11/18/20	03/01/21	
20055785	16626	Sex Offense	1	AL	12/08/20	12/30/20	06/18/21	
20055980	16624	Rape	1	CAG	12/08/20	12/29/20	05/05/21	
20056351	16407	Rape	1	HW	11/18/20	11/25/20	02/16/21	
20056415	16490	Sex Offense	1	HW	12/04/20	12/07/20	02/04/21	
20056695	16868	Carjacking	2	HW	11/19/20	02/22/21	04/26/21	
20056752	16618	Assault	2	AL	11/19/20	12/28/20	02/10/21	
20056868	16555	Homicide	2	AL	11/23/20	01/11/21	02/02/21	
20057045	16556	Homicide	3	SF	11/23/20	12/16/20	01/19/21	
20057648	16491	Rape	1	HW	12/03/20	12/07/20	02/09/21	
20058685	16658	Robbery	2	HW	12/17/20	01/08/21	02/10/21	
20058691	16492	Rape	1	HW	12/03/20	12/07/20	02/19/21	
			3	HW	12/03/20	01/11/21	02/19/21	
20058808	16864	Attempted Murder	2	HW	12/09/20	02/22/21	04/26/21	
20059087	16571	Homicide	2	VSS	12/18/20	12/18/20	02/02/21	
20059088	16680	Rape	1	RJ	12/31/20	01/08/21	03/01/21	
20059133	16834	Homicide	1	HW	01/13/21	02/16/21	04/14/21	
			2	HW	01/29/21	02/16/21	04/14/21	
20059903	16553	Assault	1	AL	12/08/20	01/11/21	01/22/21	
20060041	16865	Hit and Run	1	AL	01/19/21	02/22/21	05/07/21	
20060055	16917	Homicide	6	HW	12/16/20	03/01/21	04/20/21	
			7	HW	12/17/20	03/01/21	04/20/21	
			8	HW	02/25/21	03/01/21	04/20/21	
			9	HW	12/17/20	08/18/21	08/31/21	
			11	HW	03/25/21	03/31/21	04/19/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
20060158	17102	Weapons	2	NYN	12/10/20	04/02/21	05/03/21	
20060239	16642	Robbery	1	HW	12/23/20	01/06/21	02/09/21	
20060260	16660	Rape	1	HW	12/28/20	01/08/21	03/17/21	
20060346	17087	Assault	3	NYN	12/10/20	04/02/21	05/03/21	
20060412	17924	Assault	2	SF	03/19/21	08/18/21	12/03/21	
20060927	16662	Rape	1	AL	12/30/20	01/27/21	02/10/21	
20061418	16663	Rape	1	CAG	12/30/20	01/08/21	03/29/21	
			2	CAG	12/30/20	02/02/21	03/29/21	
20061565	16866	Homicide	3	HW	01/15/21	02/22/21	04/28/21	
20061583	16661	Rape	1	RJ	12/29/20	01/08/21	02/10/21	
20063716	17337	Assault	3	AL	01/06/21	05/06/21	06/15/21	
20063910	17346	Assault	3	AL	01/05/21	06/15/21	07/23/21	
200905	17288	Other Criminal	1	VSS	04/21/21	05/05/21	07/21/21	
			4	VSS	05/06/21	05/05/21	07/21/21	
21000009	16835	Homicide	3	HW	01/05/21	02/17/21	04/27/21	
			4	HW	02/09/21	02/17/21	04/27/21	
21000316	16691	Rape	1	SF	01/13/21	01/19/21	06/10/21	
21000541	17491	Weapons	3	SF	01/06/21	05/27/21	07/26/21	
21000730	16682	Sex Offense	1	RJ	01/06/21	01/08/21	03/01/21	
21000830	17634	Robbery	1	SF	03/31/21	07/07/21	10/13/21	
21000838	16667	Attempted Murder	1	HW	01/08/21	01/11/21	02/10/21	
			4	SF	03/31/21	07/07/21	09/23/21	
21000916	16845	Robbery	1	HW	02/11/21	02/17/21	03/17/21	
21001005	16698	Rape	1	SF	01/14/21	01/19/21	05/19/21	
21001493	17635	Homicide	1	EK	03/23/21	07/01/21	08/10/21	
21001658	16699	Rape	1	SF	01/14/21	01/19/21	03/19/21	
21001836	16739	Rape	1	VSS	01/21/21	01/27/21	04/12/21	
21002016	16738	Rape	1	VSS	01/19/21	01/27/21	04/14/21	
21002065	16826	Rape	1	AL	02/03/21	02/10/21	04/13/21	
21002412	16836	Homicide	1	HW	02/03/21	02/17/21	03/19/21	
21002569	16740	Homicide	1	VSS	01/21/21	01/27/21	03/17/21	
21002579	16846	Homicide	2	HW	02/09/21	02/17/21	03/19/21	
21002737	16793	Sex Offense	1	CAG	01/27/21	02/03/21	03/29/21	
21002740	16707	Homicide	1	HW	01/20/21	01/21/21	03/24/21	
21002803	16766	Rape	1	CAG	01/27/21	02/01/21	03/17/21	
21002982	16776	Sex Offense	1	CAG	01/28/21	02/02/21	05/11/21	
			2	CAG	06/15/21	06/15/21	09/02/21	
21003060	16825	Sex Offense	1	SF	01/29/21	02/10/21	04/12/21	
21003120	16757	Weapons	1	VSS	01/21/21	01/27/21	03/18/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21003728	16847	Weapons	2	HW	02/09/21	02/17/21	03/19/21	
21004076	17167	Assault	3	SF	02/08/21	04/13/21	06/22/21	
21004492	17168	Robbery	1	HW	02/03/21	04/13/21	06/09/21	
21005104	16824	Rape	1	SF	02/04/21	02/10/21	04/12/21	
21005639	16816	Weapons	4	NYN	02/16/21	03/30/21	05/14/21	
21005660	16863	Sex Offense	1	RJ	02/17/21	02/22/21	04/16/21	
21005856	16837	Rape	1	HW	02/09/21	02/18/21	04/14/21	
21007263	16985	Homicide	2	AL	03/16/21	03/25/21	05/10/21	
21007420	16999	Homicide	2	AL	03/12/21	05/07/21	08/10/21	
21007564	17169	Robbery	1	CAG	02/18/21	04/13/21	09/21/21	
21007594	17516	Weapons	2	CAG	03/29/21	09/03/21	12/13/21	
21007965	16961	Rape	1	VSS	03/04/21	03/09/21	04/30/21	
			2	VSS	04/06/21	04/07/21	05/07/21	
			3	VSS	07/20/21	07/20/21	09/08/21	
21008014	16960	Sex Offense	1	VSS	02/25/21	03/09/21	04/20/21	
21008066	16975	Sex Offense	1	CAG	03/10/21	03/15/21	06/28/21	
21008400	17347	Homicide	3	EK	03/01/21	05/12/21	06/15/21	
21008563	17000	Rape	1	AL	03/16/21	03/23/21	05/13/21	
21008884	17420	Homicide	3	SF	03/01/21	06/30/21	09/30/21	
21008893	17170	Homicide	2	HW	03/01/21	04/12/21	05/20/21	
21008933	16916	Homicide	1	SF	02/26/21	03/01/21	05/07/21	
			2	RJ	04/07/21	04/07/21	05/07/21	
			3	SF	04/27/21	04/27/21	05/07/21	
21009245	16986	Assault	1	CAG	03/10/21	03/15/21	06/25/21	
21009400	16976	Sex Offense	1	CAG	03/09/21	03/15/21	05/24/21	
21010069	16964	Attempted Murder	1	SF	03/04/21	03/10/21	05/14/21	
21010282	16962	Sex Offense	1	VSS	03/08/21	03/09/21	07/02/21	
			2	VSS	03/10/21	03/10/21	07/02/21	
21010400	17027	Sex Offense	1	NYN	03/24/21	03/30/21	05/13/21	
21011730	17028	Rape	1	NYN	03/24/21	03/30/21	05/14/21	
21012113	17063	Homicide	2	EK	03/23/21	07/06/21	07/27/21	
			3	EK	06/15/21	07/06/21	07/27/21	
21012315	17636	Attempted Murder	3	EK	03/23/21	07/06/21	07/27/21	
21012352	17001	Sex Offense	1	AL	03/22/21	03/23/21	05/13/21	
21012686	17133	Homicide	3	SF	04/02/21	04/12/21	07/07/21	
			4	SF	04/08/21	04/12/21	07/07/21	
21012826	17465	Assault	2	SF	03/26/21	05/25/21	07/16/21	
21012836	17044	Attempted Murder	2	CAG	03/25/21	07/23/21	09/23/21	
21012839	17211	Sex Offense	1	VSS	04/15/21	04/20/21	08/25/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21013292	17033	Attempted Murder	3	SF	05/27/21	07/22/21	11/01/21	
21013311	17132	Sex Offense	1	RJ	04/01/21	04/02/21	05/24/21	
			2	RJ	04/08/21	04/08/21	05/24/21	
21013351	17214	Homicide	4	SF	04/14/21	06/09/21	07/23/21	
			5	SF	04/22/21	06/09/21	07/23/21	
21013825	17427	Sex Offense	1	SF	05/12/21	05/19/21	07/28/21	
			2	SF	05/12/21	05/19/21	07/28/21	
21015947	17192	Homicide	1	AL	04/12/21	07/28/21	11/19/21	
21016024	17251	Sex Offense	1	CAG	04/14/21	04/26/21	06/11/21	
21016026	17315	Homicide	2	AL	04/29/21	05/04/21	07/09/21	
21016247	17196	Homicide	1	NYN	04/12/21	08/04/21	10/27/21	
21016388	17348	Rape	1	EK	05/04/21	05/13/21	06/15/21	
21016434	17351	Homicide	2	EK	05/06/21	05/10/21	05/25/21	
21016758	17260	Rape	1	CAG	04/22/21	04/27/21	06/25/21	
21016959	17261	Rape	1	CAG	04/21/21	04/27/21	06/18/21	
21017651	17317	Homicide	2	AL	04/23/21	05/04/21	06/04/21	
21017862	17269	Sex Offense	1	SF	04/21/21	04/28/21	07/19/21	
			2	SF	07/26/21	08/06/21	12/09/21	
21018029	17293	Rape	1	NYN	04/29/21	05/03/21	07/13/21	
21018445	17349	Burglary	1	EK	05/03/21	05/13/21	06/14/21	
			2	VSS	05/24/21	05/26/21	08/06/21	
21019226	17350	Rape	1	EK	05/06/21	05/13/21	06/15/21	
21019256	17430	Burglary	3	VSS	05/21/21	05/26/21	08/10/21	
21019404	17428	Rape	1	NYN	05/07/21	05/20/21	06/16/21	
21019875	17429	Rape	1	NYN	05/10/21	05/20/21	09/20/21	
21020232	17464	Sex Offense	1	SF	05/17/21	05/24/21	07/21/21	
21020353	17463	Rape	1	SF	05/12/21	05/24/21	07/27/21	
21020428	17481	Rape	1	VSS	05/26/21	05/26/21	09/03/21	
21020752	18291	Weapons	2	CAG	03/11/21	10/20/21	12/06/21	
21021725	17702		1	VSS	06/24/21	07/13/21	08/17/21	
21021747	17925	Rape	1	EK	08/06/21	08/16/21	10/14/21	
21022351	17472	Rape	1	SF	05/19/21	05/26/21	06/24/21	
21022361	17482	Rape	1	VSS	05/20/21	05/26/21	08/10/21	
			2	VSS	07/07/21	07/14/21	09/20/21	
21022554	17675	Sex Offense	1	EK	06/30/21	07/08/21	08/16/21	
21023021	17926	Homicide	1	EK	06/22/21	08/19/21	10/15/21	
21023596	17565	Rape	1	NYN	06/16/21	06/24/21	09/24/21	
21023657	17480	Sex Offense	1	VSS	05/25/21	06/10/21	07/21/21	
			4	VSS	05/26/21	05/26/21	07/21/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21023657	17480	Sex Offense	6	VSS	05/27/21	06/10/21	07/21/21	
21023776	17541	Homicide	1	AL	06/04/21	06/14/21	07/16/21	
			4	AL	08/09/21	08/11/21	10/27/21	
21023806	17556	Homicide	2	NYN	06/04/21	06/17/21	06/29/21	
21023847	17519	Rape	1	EK	05/28/21	06/08/21	09/13/21	
21024105	17696	Homicide	1	VSS	06/21/21	07/14/21	09/02/21	
			5	VSS	07/07/21	07/14/21	09/02/21	
21024541	17927	Rape	1	SF	08/12/21	08/16/21	11/19/21	
21024587	17703	Weapons	1	VSS	06/24/21	07/13/21	08/18/21	
21024838	17566	Sex Offense	1	NYN	06/17/21	06/25/21	07/26/21	
			2	NYN	06/17/21	08/06/21	10/13/21	
21025136	17602	Carjacking	2	SF	06/08/21	06/28/21	07/26/21	
			4	SF	06/24/21	06/28/21	06/29/21	
21025432	17611	Weapons	1	SF	06/04/21	06/29/21	09/22/21	
21025640	18016	Other Person	1	SF	06/10/21	08/27/21	12/03/21	
21025834	17557	Rape	1	NYN	06/10/21	06/24/21	09/20/21	
			3	NYN	07/13/21	07/15/21	09/20/21	
21026602	18025	Sex Offense	1	CAG	08/26/21	08/31/21	12/01/21	
21027249	17601	Sex Offense	1	SF	06/16/21	06/25/21	09/20/21	
21027433	17676	Rape	1	EK	06/30/21	07/08/21	08/16/21	
21027774	17853	Rape	1	SF	08/03/21	08/09/21	10/18/21	
21028801	17677	Sex Offense	1	SF	06/30/21	07/19/21	10/08/21	
21029048	17852	Rape	1	SF	08/03/21	08/09/21	10/14/21	
21029061	17750	Sex Offense	1	AL	07/06/21	07/26/21	10/04/21	
21029125	17721	Sex Offense	1	SF	07/06/21	07/19/21	11/01/21	
21029353	17715	Rape	1	VSS	07/01/21	07/16/21	09/29/21	
21029534	17855	Carjacking	2	SF	07/27/21	08/09/21	12/15/21	
21029908	17851	Kidnapping	3	AL	08/05/21	08/25/21	09/23/21	
21030018	17729	Rape	1	SF	07/06/21	07/23/21	10/06/21	
21030055	17741	Sex Offense	1	SF	07/14/21	07/22/21	09/23/21	
21030348	17850	Attempted Murder	1	SF	07/06/21	08/11/21	12/13/21	
21030428	17929	Rape	1	EK	08/05/21	08/17/21	12/27/21	
21032011	17704	Homicide	1	VSS	07/13/21	07/14/21	08/17/21	
21032314	17752	Rape	1	NYN	07/19/21	07/26/21	12/01/21	
21032706	17757	Rape	1	AL	07/15/21	07/28/21	09/03/21	
21032766	17809	Homicide	1	NYN	07/20/21	08/04/21	11/01/21	
			3	NYN	09/07/21	09/16/21	11/01/21	
21032767	17810	Homicide	2	NYN	07/20/21	08/06/21	10/08/21	
21033192	17836	Rape	1	NYN	07/26/21	08/05/21	10/05/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
21033238	17854	Rape	1	EK	08/03/21	08/09/21	10/14/21	
21033732	17837	Rape	1	NYN	07/21/21	08/05/21	10/08/21	
21035260	18024	Assault	1	CAG	08/13/21	08/30/21	11/05/21	
21036286	17965	Homicide	1	VSS	08/11/21	08/25/21	12/15/21	
21036524	18034	Sex Offense	1	CAG	08/12/21	09/01/21	12/13/21	
			2	CAG	09/02/21	09/03/21	12/13/21	
21036648	18035	Sex Offense	1	CAG	08/12/21	09/01/21	12/01/21	
21036778	17994	Rape	1	VSS	08/13/21	08/24/21	10/13/21	
21036830	17997	Sex Offense	1	VSS	08/13/21	08/24/21	12/30/21	
			2	VSS	08/24/21	08/24/21	12/30/21	
21038078	18058	Rape	1	SF	08/26/21	09/03/21	12/13/21	
21038138	18072	Rape	1	EK	08/30/21	09/07/21	12/30/21	
21038518	17975	Homicide	2	HW	08/23/21	08/25/21	10/13/21	
21039365	18164	Sex Offense	1	NYN	08/26/21	09/22/21	12/23/21	
21039732	18064	Sex Offense	1	CAG	08/26/21	09/03/21	11/19/21	
21039816	18043	Officer Involved	2	CAG	08/31/21	09/20/21	12/22/21	
21039881	18074	Rape	1	AL	08/30/21	09/07/21	10/14/21	
21039973	18161	Rape	1	SF	09/08/21	09/21/21	12/06/21	
21040919	18192	Rape	1	SF	09/02/21	09/27/21	12/13/21	
21041052	18076	Homicide	3	AL	09/03/21	09/08/21	10/13/21	
21045076	18342	Homicide	1	HW	11/05/21	11/08/21	12/07/21	
21046897	18241	Rape	1	HW	10/08/21	10/08/21	10/29/21	
21049455	18292	Attempted Murder	2	CAG	10/22/21	10/22/21	12/09/21	
			6	SF	11/01/21	11/02/21	12/08/21	
			7	SF	11/01/21	11/02/21	12/08/21	
			8	SF	11/03/21	11/03/21	12/08/21	
			10	CAG	11/22/21	11/23/21	12/30/21	
21051405	18341	Assault	1	HW	11/05/21	11/08/21	12/17/21	
70054254	16965	Cold Case	2	VSS	02/29/12	04/21/21	09/29/21	
84007346	17057	Homicide	2	RJ	02/17/21	03/31/21	05/17/21	
90080996	17188	Rape	1	SF	09/25/20	04/15/21	06/29/21	
90111076	17453	Rape	1	SF	09/25/20	05/24/21	08/05/21	
91004254	17189	Rape	1	CAG	08/27/20	04/15/21	06/28/21	
91025384	17190	Rape	1	SF	08/27/20	04/15/21	06/29/21	
91032319	17191	Rape	1	AL	09/01/20	06/08/21	06/23/21	
91049814	17234	Rape	1	VSS	09/25/20	04/22/21	05/26/21	
91100433	17294	Rape	1	AL	09/29/20	05/03/21	06/02/21	
91116792	17233	Rape	1	VSS	09/29/20	04/22/21	05/24/21	
91133790	17295	Rape	1	AL	09/01/20	05/03/21	06/11/21	

Unit FB

RD No	Lab No	Crime Type	No.	Analyst	Request	Assigned	Completed	Cancelled
91138313	17296	Rape	1	AL	09/01/20	05/03/21	06/03/21	
93115065	17341	Rape	1	EK	09/02/20	06/08/21	09/08/21	
94087483	16402	Homicide	1	HW	11/03/20	11/23/20	02/09/21	
95065901	17525	Rape	1	CAG	09/02/20	06/08/21	08/09/21	
97098610	17963	Rape	1	EK	09/03/20	08/19/21	10/15/21	
98079335	16501	Cold Case	1	SF	10/27/20	12/07/20	04/13/21	

430 requests for 218 new cases completed.

430 requests and 218 new cases completed.