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 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 December meeting minutes

4. Open Forum/Public Comment

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

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

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

December 2, 2021 5:00 PM
Teleconference
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**: Vacant*

1. Call to Order, determination of quorum

Members Present: Hofer, Gage, Katz, Oliver, De La Cruz, Brown, Sulieman, and Tomlinson.

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

The resolution passed unanimously.

3. Review and approval of the draft November meeting minutes

The November Minutes passed unanimously.

4. Open Forum/Public Comment

There was one Public Speaker under Open Forum:
Assata Olugbala spoke about a Homelessness Intervention on East 12th Street that she believes creates a privacy concern due to the manner in which the intervention is divided and managed.

5. Surveillance Equipment Ordinance – DPW – Illegal Dumping Camera Proposal
    a. Review and take possible action on Impact Report and proposed Use Policy

Vice Chair Gage introduced this item with some framing remarks about the process of the ad hoc committee working with staff to refine what was originally brought forward and stated that the proposal before the PAC represented a good balance between the public need to address illegal dumping and civil

liberties. He indicated that the ad hoc members were recommending support by the full PAC. Member Suleiman added that she really appreciated the staff decision to switch vendors in order to address the concerns of the PAC. Member Katz, also from the ad hoc, also weighed in with his support.

Victoria Chak from OPW presented the Impact Statement and Use Policy with support from Marcel Corby who represents the selected vendor of the technology. She touched on key components including data retention and sharing, the ability of the cameras to focus their surveillance area to the public right-of-way, and the who will have access to the footage and how they will be trained.

Member De La Cruz asked for more details on when OPD would have access to the cameras and Victoria explained that the Use Policy allows for a reporting mechanism to the PAC when OPD requests data and also clarifies when OPW staff can download footage if it captures evidence of certain types of serious, violent crimes. Member Oliver had questions about access to the camera "pods" and router and Wi-Fi security questions.

Member Brown asked if staff could commit in the Use Policy to using the blocking technology to ensure that only the public right-of-way is captured on camera. After some discussion, language was offered to ensure this.

A motion was proposed by Member Sulieman with additional language form Vice Char Gage that inserted two amendments to cover OPD access and the blocking of areas outside the right-of-way. The motion passed unanimously.

Chair Hofer invited Rosa Velasquez from Council Member Treva Reid's Office to address the PAC. She highlighted the importance of this issue to her district, citing the epidemic that it is and the impact it has on vulnerable neighborhoods they represent. She thanked the PAC for their work and expressed her support for their recommendation to approve the use of this technology.

The Chair then opened the floor to public comment and there were 10 speakers:

Jonathan Randolph indicated his support for the use of the cameras and noted that illegal dumping is horrendous in his neighborhood. He also raised concern about data security once downloaded to a device.

Oscar Yassin noted that he had watched this process unfold and was very pleased that OPW took the time to work with the ad hoc and changed vendors when the first was problematic, noting this is an example of how the process is supposed to work. He also aired concern that his Council Member was pushing for a faster process which may have resulted in the use of that vendor.

Sharoane Allen raised a concern about theft or vandalism to the cameras and also asked it they could be used to enforce parking rules if people are observed in violation with the cameras.

Billie Jean Carter stated support for the program and also has concerns about vandalism of the cameras. She also raised concern about a short retention period in case the cameras caught footage of a major crime.

Assata Olugbala stated that illegal dumping is enormous and that something definitely needs to be done. She also praised the PAC for how it does its work, noting that its process holds the City accountable and leads to a better outcome.

Sarah LaRock spoke on behalf of Waste Management noting that their crews spend a huge amount of time addressing illegal dumping in Oakland and that this was a great step to addressing the issue.

Mrs. West (first name unknown) spoke about efforts with the Beat 31y Neighborhood Council trying to clean up their neighborhood and noted that its important for the City to go after the dumpers and not just pick up the dumping if this problem is going to be solved.

Mary Forte spoke about her decades of experience picking up illegal dumping and litter in Council District 7 and the need to build evidence against the dumpers to bring good cases forward. She feels the dumpers have invaded her privacy, trashed her neighborhood, and reduced her quality of life.

Allyce Sandbach spoke on behalf of the Alameda County District Attorney's Office in which she serves as an Environmental Prosecutor. She aired her appreciation for the process and stated that she believes the cameras are absolutely necessary because her office has been limited in prosecuting dumpers due to a lack of solid evidence that a camera can provide. She also stated that she believes the cameras will provide some communities with hope that something can be done and will change.

Ernestine Wilson with Faith in Action East Bay noted that 1000's of people in Oakland have fought for this and they deserve some relief in their community.

Vice Chair Gage made a motion to recommend to the City Council that it adopt the Use Policy with the addition of the two amendments. The motion was seconded by Chair Hofer and passed unanimously.

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 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
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 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.

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:** 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 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:** 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

Surveillance Impact Report:
CrimeView Product Suite

A. Description: The CrimeView Product Suite and Function

The CentralSquare 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. 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. 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. This application complements the City's already existing IDT-based CrimeWatch open-data initiative.

B. Proposed Purpose

CentralSquare's CrimeView product suite (see ***Attachment A*** 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.

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[1]) 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[2]) 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] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54
[2] https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=

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 (see ***Attachment B***) "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 C***) provides more security standards.

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.
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 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[3]. 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 Cybersecurity Program Overview and CentralSquare's Analytics Product

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

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).

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.

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 California use the CrimeView product suite, including, including 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.

CENTRALSQUARE

Attachment A
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.

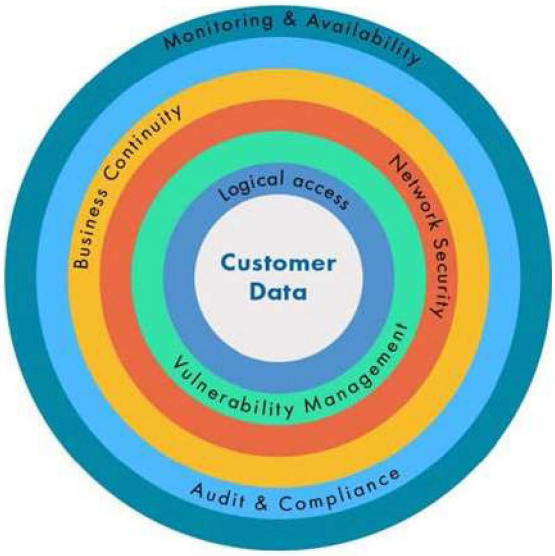
- Business Impact Analysis (BIA).
- Business Continuity Plan (BCP)
- Defined SLAs (Service Level Agreement), RTOs (Recovery Time Objective) and RPOs (Recovery Point Objective).
- Annual Disaster Recovery tests and/or Tabletop exercises, to include validation of recovered environment.
- Training and Annual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

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