DEPARTMENTAL GENERAL ORDER

I 29: CRIME ANALYSIS SOFTWARE

Effective Date:

Coordinator: Criminal Investigations Division, Crime Analysis Unit

CRIME ANALYSIS SOFTWARE

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

A. VALUE STATEMENT

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

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

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

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

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

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

CentralSquare's CrimeView product suite comprises three applications:

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

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

[1] OPD relies on CentralSquare's CrimeView at the time of the production of this policy for its crime analysis software needs. OPD may choose a different crime analysis software vendor in the future as technology and OPD Crime Analysis Section needs evolve over time. Any new software product must first be submitted for approval per O.M.C. 9.64 et seq.

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

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

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

This product suite does not contain a predictive component. It is used to assist experienced and trained crime analysts create informed analytical commentary supplemented by temporal and visual information. This information helps OPD commanders make sense of the tremendous amount of crime data generated in Oakland.

D. **Authorized Use**: *the specific uses that are authorized, and the rules and processes required prior to such use the information that can be collected by the surveillance technology.*

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

CrimeView Desktop – This application is a license-based desktop application that is used only by trained and experienced crime analysts. The application is an extension to ESRI's ArcGIS enterprise mapping program. Each crime analyst has ArcGIS installed on his or her computer. The CrimeView Desktop extension is then installed by CentralSquare technicians. Only authorized users may have this application installed on their desktops; all OPD desktop machines require a unique username and password for access. Analysts use the software to manually identify trends, patterns, and areas with high concentrations of specific crimes.

CrimeView Analytics – This application is an OPD-wide SaaS application. Only OPD sworn law enforcement personnel or authorized professional staff may access CrimeView Analytics. Users must be employees of OPD and have passed all appropriate background checks and clearances. CrimeView Analytics users must access the system using a unique username and password. Access is granted and managed by CID management personnel. OPD personnel use the software to manually identify trends, patterns, and areas with high concentrations of specific crimes.

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

Users shall not use or let others use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to

[5] https://www.courts.ca.gov/4901.htm

[6] https://irp.fas.org/agency/doj/fbi/is/ncic.htm

[7] https://www.nlets.org/

authorized investigations, internal audits, or for crime analysts to produce crime analysis reports.

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

CrimeView Desktop – Authorized users include only (CID commander) approved crime analysts.

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

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

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

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

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

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

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

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

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

Crimemapping.com is the current name of the public facing component of the CrimeView product suite. This public portal provides the public with a map-based view of crime incidents in the City of Oakland.

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

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

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

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

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

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

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

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

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

Specifically, the training includes the following:

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

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

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

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

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

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

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

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

By Order of

LeRonne L. Armstrong

Chief of Police   Date Signed: