



Privacy Advisory Commission
March 9, 2017 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
Special Meeting Agenda

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: Yaman Salahi, District 3 Representative: Brian M. Hofer, District 4 Representative: Lou Katz, District 5 Representative: Raymundo Jacquez III, District 6 Representative: Clint M. Johnson, District 7 Representative: Robert Oliver, Council At-Large Representative: Saied R. Karamooz, Mayoral Representative: Deirdre Mulligan.*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:00pm: Call to Order, determination of quorum.
2. 5:05pm: Review and approval of February 2 meeting minutes.
3. 5:10pm: Presentation and possible action on proposed "Civil Rights Ordinance" (Councilmember McElhaney) – guest speakers Christina Sinha (AAAJ-ALC), John Crew (Police Practices Expert), Brittney Rezaei (CAIR-SFBA), Pastor Michael McBride (PICO), Matt Cagle (ACLU).
4. 6:00pm: Presentation and possible action on Surveillance Equipment Ordinance Sections 8, 9, 10 (City Attorney's office)
5. 6:30pm: Presentation and discussion on data sharing/joint operation agreements (Oakland Police Department). No action will be taken on these items at this meeting.
6. 6:40pm: Open Forum
7. 6:45pm: Adjournment



Privacy Advisory Commission
February 2, 2017 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

Commission Members: *District 1 Representative: Reem Suleiman, District 2 Representative: Yaman Salahi, District 3 Representative: Brian M. Hofer, District 4 Representative: Lou Katz, District 5 Representative: Raymundo Jacquez III, District 6 Representative: Clint M. Johnson, District 7 Representative: Robert Oliver, Council At-Large Representative: Saied R. Karamooz, Mayoral Representative: Deirdre Mulligan.*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:00pm: Call to Order, determination of quorum.

All members were present.

2. 5:05pm: Review and approval of January 5 meeting minutes.

The January Minutes were approved unanimously.

3. 5:10pm: Presentation on Automated License Plate Readers by Oakland Police Department.

Captain Figueroa with OPD provided a brief overview of the ALPR system. He explained that the data is managed by the vendor and that each police vehicle that has an ALPR also has a computer that receives three downloads from the DMV daily: Felony Warrants, Stolen Vehicles, and Stolen License Plates. There are 35 cars with APLRs with two cameras each. Each camera takes a color photo and an infrared photo of the plate. When the photo is taken the computer compares it to the database and then alerts the officer when it finds a match. He also explained the City has a desktop application in which they can search a plate and determine if it was recently detected.

4. 5:20pm: Presentation on Automated License Plate Readers by Cyrus Farivar, Senior Business Editor at Ars Technica.

Cyrus Farivar presented his story as a journalist who requested and received the Oakland ALPR database through a records request and received it. He noted that he made the same request of several other jurisdictions but only Oakland was responsive. He went on to note that Oakland did not have a data retention policy at the time of his request but since has implemented a 6 month policy. He noted that most people have no understanding of how departments use ALPRs nor what policies should guide them.

5. 5:30pm: Presentation on Automated License Plate Readers by Mike Katz-Lacabe, Director of Research at Center for Human Rights and Privacy.

Mike Katz-Lacabe presented on his experience in San Leandro and drew a comparison to Oakland. San Leandro has three cameras on each car which is why an ALPR equipped San Leandro Police Car captured a picture of him and his daughter in the driveway as they were unloading groceries. Oakland has only two cameras and they are pointed in a manner to prevent images being captured that are off the street. He further noted that ALPRs can be placed on trailers that can be moved around and appear to be trailers telling drivers how fast they are going (while also capturing their photo and license plate info). He noted that the federal government has three of these locally through their Northern CA Regional Intelligence Center (NCRIC) and that the Contra Costa Sheriff's Office has one.

He went on to point out that often these ALPRs have misreads which can cause situations where law enforcement officials pull over the wrong person (and in at least one case drew their guns on an innocent person whose plate was misread by the ALPR).

Many local jurisdictions send all their data from ALPRs to NCRIC, however, Oakland does not. The federal government has no data retention limit, the CA Highway Patrol has a 60 day limit, and Oakland's is 6 months. When NCRIC receives data from local jurisdictions they keep it for a year. Once NCRIC has it, it can be shared with many agencies such as BART, ICE, or the Department of Insurance.

6. 5:40pm: Review and discuss current Oakland Police Department Automated License Plate Reader policy. No action on this item will be taken at this meeting.

Chairperson Hofer opened up this portion of the discussion with questions about OPD's Data Sharing Agreements. Captain Figueroa stated that the City has one with Aries which connects to Alameda and Contra Costa Sheriff's Offices and with LEAP. The City does NOT have a sharing agreement with NCRIC.

Member Salahi asked about sharing directly with other local law enforcement agencies and Captain Figueroa, referencing Government Code 430.9 noted that the department will only share for law enforcement purposes and that there are very few requests he is aware of. However, if the data is shared through LEAP or Aries, then OPD would not be aware of another agency using the data.

Tim Birch from OPD noted that the 6 month retention period the department currently uses may not be a sufficient window of opportunity due to current staffing in investigations—Oakland has a very high number of violent crimes per 100,000 people compared to other cities—Oakland has 10 per 100K whereas the national average is 4. This means it takes longer for the City to investigate and he is recommending a one year retention policy.

Member Mulligan asked about the effectiveness of ALPRs in solving violent crimes—DC Lois did not have data on this but suggested it could be researched. She also raised the concern about the access to the

database, especially since it is maintained by an outside vendor. However, she also asked if the database would be available to Public Defenders because there could possibly be exculpatory data captured as well as incriminating data. Member Saied asked if ALPRs were an acceptable replacement for Oakland's staffing shortage and if alternative methods would be more effective.

Member Jaquez raised concerns about the efficacy of using ALPRs especially if they often make an inaccurate read. He also was worried about the third party access to the info and if it could be used to impact someone's civil liberties by building a profile of the person based on where they travel and are detected by ALPRs. It was asked if ICE has requested any data yet (and they have not).

Member Sulliman suggested the Commission could draft language that would limit the City's honoring requests from Federal Agencies in light of the new administration's tactics regarding immigration.

7. 6:15pm: Open Forum

Brian Geiser noted that ALPRs are used by more than just OPD—at the last meeting the City's Public Works Department was discussing their use for Neighborhood Parking Management. He also stated he thinks the City should ban third party contractors from using ALPRs in Oakland.

8. 7:00pm: Adjournment

THE SURVEILLANCE AND COMMUNITY SAFETY ORDINANCE

Whereas, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology; and

Whereas, the City Council finds that, while surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

Whereas, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes, while acknowledging the significance of protecting the privacy of citizens; and

Whereas, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

Whereas, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

Whereas, the City Council finds that any and all decisions regarding if and how surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight; and

Whereas, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

Whereas, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to; now, therefore

THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. City Council Approval Requirement

- 1) A City entity shall notify the Chair of the Privacy Advisory Commission prior to the entity:
 - a) Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - b) Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

Upon notification by the entity, the Chair shall place the item on the agenda at the next meeting for discussion and possible action. At this meeting, the entity shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action the entity intends to take. The Privacy Advisory Commission may vote its approval to proceed, object to the proposal, recommend that the entity modify its proposal, or take no action. Failure by the Privacy Advisory Commission to act shall not prohibit the entity from proceeding. Opposition to the action by the Privacy Advisory Commission shall not prohibit the entity from proceeding. The City entity is still bound by subsection (2) regardless of the action taken by the Privacy Advisory Commission under this subsection.

- 2) A City entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public hearing prior to any of the following:
 - a) Accepting state or federal funds or in-kind or other donations for surveillance technology;
 - b) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
 - c) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council; or
 - d) Entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides
- 3) A City entity must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (2)(a)-(d).

Section 3. Information Required

- 1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
 - a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use

Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting.

- b) The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose modifications to the City entity and/or City Council in writing.
 - c) Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.
- 2) After receiving the recommendation of the Privacy Advisory Commission, the City Council shall provide the public notice that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.
 - 3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 4. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 5. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy for each surveillance technology, in compliance with Section 3 (1) (a-c).

- a) Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, each City entity shall present to the Privacy Advisory Commission a list of surveillance technology already possessed or used by the City entity.
- b) The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
- c) Within sixty (60) days of the Privacy Advisory Commission's action in b), each City entity shall submit at least one (1) Surveillance Impact Report

and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter every month until the list is exhausted.

- d) Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following City Council Approval

- 1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.
 - a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Privacy Advisory Commission for its review.
 - b) The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.
- 2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.
- 3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
 - a) A summary of all requests for City Council approval pursuant to Section 2 or Section 5 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
 - b) All Surveillance Reports submitted.

Section 7. Definitions

The following definitions apply to this Ordinance:

- 1) "Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
 - a) A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
 - b) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau;
 - e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public's civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
 - f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
 - g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - i) Statistics and information about public records act requests, including response rates;
 - j) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
 - k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
- 2) "City entity" means any department, bureau, division, or unit of the City of Oakland.
- 3) "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal,

olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.

- a) "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 7(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
- 4) "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:
 - a) **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
 - c) **Location:** The location(s) it may be deployed and crime statistics for any location(s);
 - d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;
 - e) **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
 - f) **Data Types and Sources:** A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
 - g) **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

- h) **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
 - i) **Third Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
 - j) **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
 - k) **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).
- 5) "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- a) **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
 - b) **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;
 - c) **Data Collection:** 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;
 - d) **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
 - e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
 - f) **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;
 - g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;

- h) **Third Party Data Sharing:** If and how other City 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;
- i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;
- j) **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; and
- k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section 8. Enforcement

- 1) Any violation of Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), Resolution No. ~~xxxxx~~86505 (Cell Site Simulator Use Policy adopted ~~xxxxxx~~February 7, 2017), this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city agency, the City of Oakland, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third-party with possession, custody, or control of data subject to this Ordinance.
- ~~2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater) and punitive damages.~~
- 2) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) ~~or (2)~~.
- 3) Any violation committed by a City employee of Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR

Surveillance Use Policy adopted October 6, 2015), Resolution No. ~~xxxxx~~86505 (Cell Site Simulator Use Policy adopted ~~xxxxx~~February 7, 2017), this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, shall result in consequences that may include but are not limited to retraining, counseling, written reprimand, suspension, and/or termination of City employment.

- 4) ~~In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$1,000 per violation.~~

Section 9. Secrecy of Surveillance Technology

It shall be unlawful for the City of Oakland or any municipal entity to enter into any contract or other agreement that conflicts with the public noticing and/or transparency provisions requirements of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements provisions, shall be deemed void and legally unenforceable. Likewise ~~Conflicting any~~ provisions in contracts or agreements signed prior to the enactment of this Ordinance that conflict with the public noticing and/or transparency requirements of this ordinance, shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Ordinance.

Section 10. Whistleblower Protections.

1) ~~No municipal entity~~Neither the City nor anyone acting on behalf of ~~a municipal entity~~the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and, conditions of employment, access to information, restrictions on due process rights, ~~privileges of employment~~, or civil or criminal liability, because:

a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or

b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.

2) It shall be grounds for disciplinary action for a ~~municipal City~~ employee or anyone else acting on behalf of ~~a municipal entity~~the City to retaliate against ~~an individual~~another City employee or applicant -who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.

3) Any employee or applicant who is injured by a violation of Section 10 may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

Section 11. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].



AUTOMATED REGIONAL INFORMATION EXCHANGE SYSTEM

A PUBLIC SAFETY DATA SHARING SERVICE PROVIDED BY CONTRA COSTA COUNTY

Contra Costa County

Sheriff
Antioch PD
BART PD
Brentwood PD
Clayton PD
Concord PD
CCC Animal Services
CCC College Dist PD
CCC District Attorney
CCC EHSD Fraud
CCC Probation
CCC Superior Court
Danville PD
EBRP District PD
El Cerrito PD
Hercules PD
Kensington PD
Lafayette PD
Martinez PD
Moraga PD
Oakley PD
Orinda PD
Pinole PD
Pittsburg PD
Pleasant Hill PD
Richmond PD
San Pablo PD
San Ramon PD
Walnut Creek PD

Alameda County

Sheriff
Dublin PD
Oakland PD

Solano County

Sheriff
Benicia PD
Dixon PD
Fairfield PD
Rio Vista PD
Suisun City PD
Vacaville PD
Vallejo PD

San Joaquin County

Sheriff
Escalon PD
Lathrop PD
Lodi PD
Manteca PD
Ripon PD
Stockton PD
Tracy PD

Santa Clara County

Sheriff
Sunnyvale PD

Dear Chief/Sheriff XXXXX,

As many of you are aware, ARIES is currently in the process of sharing the data contained within our East Bay Data Warehouse with the NCRIC. This data will then be shared with Coplink and California SmartJustice.

As part of this data sharing effort with California SmartJustice, an Interconnection Agreement must be signed by each Agency Head. This agreement is required for the agencies that are going to share data to Smart Justice thru ARIES and NCRIC. An agency user agreement is required for every agency who will be accessing the California SmartJustice system. The agency is required to sign on behalf of their users. This user agreement satisfies the legal and liability requirements for California SmartJustice. By agreeing to this, your agency will be granted access to the SmartJustice data sharing platform. A link to California SmartJustice will be available through ARIES.

During a recent ARIES Committee meeting, Department Representatives within the ARIES group approved the use of ARIES to be the conduit for sharing data with California SmartJustice, rather than each agency establishing its own connection.

As many of you know, California SmartJustice is a new criminal justice data sharing platform currently being offered by the California Attorney General's Office, Department of Justice.

Enclosed is the Interconnection Agreement along with signature page. I have also included a self-addressed envelope for your convenience. Once the agreement has been returned to me, I will ensure it is processed properly.

Sincerely,

Lieutenant Jason Vorhauer,
Office of the Sheriff, Contra Costa County
ARIES Manager



C A L I F O R N I A
SMARTJUSTICE

Interconnection Agreement

Contents

1	Purpose.....	3
2	Background.....	3
3	Definitions	3
4	Responsibilities.....	3
5	Information ownership and release	3
6	Term	4
7	Other.....	4

1 Purpose

This Interconnection Agreement (ICA) is entered into by and between the California Department of Justice (DOJ), and _____ (hereinafter referred to as "agency"), to define the relationship between DOJ and the agency as it relates to the sharing of data between DOJ and the agency.

2 Background

The public safety community is faced with the challenge of easily and accurately monitoring and tracking offender status, statewide. The passage of the Criminal Justice Realignment Act of 2011 (Chapter 15, Statutes of 2011 - Assembly Bill 109), has increased the necessity for data sharing between counties and among law enforcement and public safety agencies. These agencies need the ability to identify offenders returning to their jurisdictions and easily access complete offender profiles. Access to this data will enable agencies to effectively supervise individuals, measure outcomes of re-entry programs and offender services, and properly manage resources. Law enforcement officials who encounter these individuals must have access to up-to-date offender records and conditions of supervision, including information regarding alternative custody arrangements.

3 Definitions

1. All references to "agency" in this ICA shall be deemed a reference to "any agency."
2. All references to "instance" in this ICA shall be deemed a reference to the DOJ SmartJustice.
3. All references to "source agency" in this ICA shall be deemed a reference to the agency that contributed the information to the instance.

4 Responsibilities

1. To provide data to the maximum extent permitted by law, in a mutually agreed upon electronic format.
2. To contribute data and grant view-only access to the instance's participating agencies.
3. Such information may include, but is not limited to, record/case/jail management systems, Supervised Release File, Automated Criminal History System or other DOJ or agency owned information.
4. Compliance with the SmartJustice Policies, Practices and Procedures. For reference, see the following URL: <http://clew.doj.ca.gov/>

5 Information ownership and release

1. Ownership - Each contributing agency retains control of all information they provide through the instance at all times. An agency is responsible for creating, updating, and deleting records in its system according to its policies. An agency shall ensure the completeness and accuracy of its source data. The information contributed into the instance shall remain the property of the contributing agency.

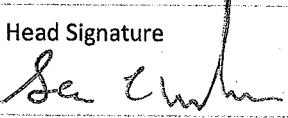
2. Referral of Information Requests from Third Parties - Any third party request for information authored or originated by another source agency shall be immediately referred to the source agency.
3. Prohibition Against Release of Information to Third Parties - The agency shall not release or make available any information it has accessed to any third party, unless they are the source agency, or as required by law.
4. Subpoenas and Court Orders - The agency may respond to a subpoena or court order for information authored or originated by another source agency after providing the source agency the opportunity to object. The agency shall immediately provide a copy of the subpoena or court order to the source agency.
5. State or Federal Public Record Requests - Upon receipt of a state or federal public record request for information authored or originated by another source agency the agency shall respond to the request by stating that the request will be referred to the source agency for response.

6 Term

This ICA may be terminated upon a 10 working day notice by either agency. In the event of a security incident that necessitates an immediate response, the 10 working day notice is not applicable.

7 Other

1. Should a conflict arise, the agency agrees to fully cooperate and provide all source documents, or other information necessary for investigation.
2. The parties agree this ICA is subject to all applicable federal, state, and local statutes, ordinances, and regulations.
3. An agency is authorized to download their own agency data from the instance.

Agency Head Signature 	Date 1-14-15
Agency Head (Printed) Sean Whent	
DOJ Signature	Date
DOJ (Printed)	



C A L I F O R N I A **SMARTJUSTICE**

Agency User Agreement

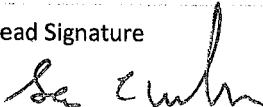
Agency Name

Agency ORI

Hereinafter referred to as the "subscriber," your agency agrees to conform to the California Department of Justice's (CalDOJ) SmartJustice Policies, Practices and Procedures (PPPs). Wherein SmartJustice information and images are classified as criminal offender record information (CORI), the subscriber agrees to conform to all CORI laws, regulations and policies. The subscriber additionally agrees to conform to all Cal-PHOTO Policies, Practices and Procedures. Accordingly, SmartJustice information and images are confidential and are to be used for law enforcement or criminal justice purposes only.

It is understood by the subscriber that violation of this Agency User Agreement may result in suspension or revocation of SmartJustice access, as deemed appropriate by the DOJ. In signing this Agency User Agreement, the subscriber is certifying that he/she is a regularly employed peace officer or other law enforcement or criminal justice agency representative. All SmartJustice users (i.e., computer operators, peace officers, investigators, analysts, agency management/supervisors, etc.) must be trained in the operation, policies, and procedures of SmartJustice. The subscriber understands that training can only be provided by DOJ's training staff, the SmartJustice Agency Coordinator (AC), or through the agency's own training program.

The CalDOJ, and/or the SmartJustice AC will perform audits on the use of the system and its records to ensure compliance with the SmartJustice PPPs. Periodic, unannounced site inspections may be performed by the CalDOJ to ensure compliance with the above.

Agency Head Signature 	Date 1-14-15
Agency Head (Printed) Sean Whelan	
DOJ Signature	Date
DOJ (Printed)	



DEPARTMENTAL
GENERAL
ORDER

28 Jun 99

M-17

Index as:

Ref:
CALEA Standard
Chapter 51

Criminal Intelligence
Intelligence, Criminal

CRIMINAL INTELLIGENCE

The purpose of this new order is to establish Departmental procedures governing the function of the Intelligence Division.

I. DEPARTMENTAL POLICY

Information gathering is a fundamental and essential element in the prevention of crime and apprehension of offenders. The policy of the Department is to gather information directed toward specific individuals or organizations reasonably suspected of criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals as defined. While criminal intelligence may be assigned to specific personnel within the Department, all members of the Department are responsible for reporting information that may help identify criminal conspirators and perpetrators.

II. DEFINITIONS

- A. Criminal intelligence is information compiled, analyzed and/or disseminated in an effort to anticipate, prevent or monitor criminal activity.
- B. Strategic intelligence is information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies for both short and long-term investigative goals.
- C. Tactical intelligence is information regarding a specific criminal event that can be used immediately by operational units to further a

criminal investigation, plan tactical operations and provide for officer safety.

III. MISSION

- A. It is the mission of the Intelligence Division to gather information from all sources, in a manner consistent with the law, in support of efforts to provide tactical or strategic information on the existence, identities, and capabilities of criminal suspects and enterprises generally and, in particular, to further crime prevention and enforcement objectives/priorities identified by the Department.
- B. Information gathering in support of the intelligence function is the responsibility of each member of the Department.
- C. Information that implicates, or suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to the Chief of Police.

IV. ORGANIZATION

- A. The Intelligence Division shall have the primary responsibility for the direction of intelligence operations, coordination of personnel, and the collection, evaluation, collation, analysis and dissemination of intelligence information.
- B. The Intelligence Division Sergeant shall report directly to the Chief of Police in a manner and on a schedule prescribed by him/her.
- C. To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the Intelligence Division Sergeant shall ensure compliance with the policies, procedures, mission and goals of the Department.
- D. Assignments of personnel to the Intelligence Division are at the sole discretion of the Chief of Police.

V. PROFESSIONAL STANDARDS

- A. The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of the individuals. To this end, members of the Department shall adhere to the following:
 - 1. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable indication that a crime has been committed or is being planned.
 - 2. Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent the criminal act and/or identify and prosecute violators.
 - 3. Members of the Intelligence Division shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the Intelligence Division.
 - 4. Information gathered and maintained by the Intelligence Division for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this order. A record shall be kept regarding the dissemination of all such information to persons within this or any other law enforcement agency.

VI. COMPILING INTELLIGENCE

- A. The Intelligence Division Sergeant, with sufficient information and justification, may open intelligence investigations/files. This includes, but is not limited to, the following types of information:

1. Subject, victim(s) and complainant as appropriate.
 2. Summary of suspected criminal activity.
 3. Anticipated investigative steps to include proposed use of informants, photographic or electronic surveillance.
 4. Resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc.
 5. Anticipated results and problems, restraints or conflicts of interest.
- B. Members shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the Intelligence Division.
- C. Information gathering using confidential informants as well as electronic, photographic and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by the Department.
- D. All information designated for use by the Intelligence Division shall be submitted on the designated report form and reviewed by the Intelligence Division Sergeant prior to submission.

VII. RECEIPT/EVALUATION OF INFORMATION

Upon receipt of information in any form, the Intelligence Division Sergeant shall ensure that the following steps are taken:

- A. Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information, where known.
- B. Reports and other investigative material and information submitted by other agencies shall remain the property of the originating

agency, but may be retained by the Department. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.

- C. Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or figures emerge.

VIII. FILE STATUS

- A. Intelligence file status will be classified as either “open” or “closed,” in accordance with the following:
 - 1. Intelligence files that are actively being worked will be designated as “open.” In order to remain open, members working such cases must file intelligence status reports at least every 180 days.
 - 2. “Closed” intelligence files are those in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files must include a final case summary report prepared by or with the authorization of the lead investigator.
- B. Classification/Security of Intelligence
 - 1. Intelligence files will be classified in order to protect sources, investigations and individual’s rights to privacy, as well as to provide a structure that will enable the Department to control access to intelligence. These classifications shall be re-evaluated whenever new information is added to an existing intelligence file.
 - a. Restricted intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers,

informants or others and/or compromise their identities. Restricted intelligence may only be released by approval of the Intelligence Division Sergeant or the Chief of Police to authorized law enforcement agencies with a need and a right to know.

- b. Confidential intelligence is less sensitive than restricted intelligence. It may be released to Department members when the Intelligence Division Sergeant or his/her designate has established that the member has a need and a right to know.
 - c. Unclassified intelligence contains information from the news media, public records and other sources of a topical nature. Access is limited to members conducting authorized investigations that necessitate this information.
2. All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the Intelligence Division Sergeant.
- a. Informant files shall be maintained separately from intelligence files.
 - b. Intelligence files shall be maintained in accordance with state and federal law.
 - c. Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the express approval of the Intelligence Division Sergeant and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of the Intelligence Division Sergeant.

- d. All files released under freedom of information provisions or through disclosure shall be carefully reviewed.

IX. AUDITING AND PURGING FILES

- A. The Intelligence Division Sergeant is responsible for ensuring that files are maintained in accordance with the goals and objectives of the Department and include information that is both timely and relevant. The Intelligence Division Sergeant shall audit and purge pertinent intelligence files on an annual basis.
- B. When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. The Intelligence Division shall maintain a record of purged files.

X. UNDERCOVER FUNDS

The Intelligence Division Sergeant may hold funds for undercover expenses in the amounts authorized by the Police Operations Imprest Account. All funds shall be maintained in a secure place within the Division. Undercover funds shall be accounted for in accordance with the provisions of [Departmental General Order F-5, UNDERCOVER EXPENDITURES](#).

By order of

Joseph Samuels, Jr.
Chief of Police

GO44/M-17



DEPARTMENTAL
GENERAL
ORDER

New Order
Effective Date
15 Nov 04

M-19

Index as:

Bias-Based Policing
Prohibitions Regarding Racial Profiling
and Other Bias-Based Policing
Racial Profiling

**PROHIBITIONS REGARDING RACIAL PROFILING AND
OTHER BIAS-BASED POLICING**

I. PURPOSE

- A. The purpose of this policy is to reaffirm the Oakland Police Department's commitment to providing service and enforcing laws in a fair and equitable manner, and to establish a relationship with the community based on trust and respect. Whenever our practices are, or are perceived to be, biased, unfair, or disrespectful, we lose public trust and support and diminish our effectiveness.
- B. The Department recognizes that there has been a growing national perception that law enforcement action is too often based on racial stereotypes ("racial profiling") or other bias-based policing – whether it is against African Americans, Latinos, Asians, Middle Easterners, South Asians, or any other race, ethnicity, national origin, gender, age, religion, sexual orientation, or disability. In Oakland, there is concern within our communities that some members may engage in this behavior. Whether individual members agree or not, we, as an organization, must recognize that this concern exists and be responsive to it.
- C. California Penal Code Section 13519.4(e) prohibits racial profiling by law enforcement officers. This Department policy explicitly prohibits racial profiling and other bias-based policing. It also states the limited circumstances in which members can consider race, ethnicity, national origin, gender, age, religion, sexual orientation, or disability in making law enforcement decisions and actions.

II. DEFINITION OF RACIAL PROFILING

The use of race, ethnicity, or national origin in determining reasonable suspicion, probable cause or the focus or scope of any police action that directly or indirectly imposes on the freedoms or free movement of any person, unless the use of race, ethnicity, or national origin is used as part of a specific suspect description.

III. POLICY

- A. Investigative detentions, traffic stops, arrests, searches and property seizures by officers shall be based on a standard of reasonable suspicion or probable cause in accordance with the Fourth Amendment of the U.S. Constitution.
- B. Members shall articulate specific facts and circumstances that support reasonable suspicion or probable cause for investigative detentions, pedestrian, bicycle, or vehicle stops, arrests, non-consensual searches and property seizures.
- C. Members shall not consider actual or perceived race, ethnicity, national origin, gender, age, religion, sexual orientation, or disability in establishing either reasonable suspicion or probable cause or when carrying out law enforcement activities EXCEPT when credible and reliable information links specific suspect descriptions to specific unlawful or suspicious activity.

Members seeking one or more specific persons who have been identified or described in part by any of the above listed characteristics may rely on these characteristics in part and only in combination with other appropriate factors.

IV. CONSENT SEARCHES

- A. A consent search refers to searches conducted not based on probable cause, incident to arrest or pursuant to a search warrant, but based on permission granted from the person being searched.
- B. Consent searches are permissible law enforcement tools; however, their use shall not be:

1. Arbitrary. In other words, the request to conduct a consent search must be reasonable and members should be able to articulate the suspicion that formed the basis for the request.
 2. Based on actual or perceived race, ethnicity, national origin, gender, age, religion, sexual orientation, or disability.
- C. Members shall complete a Field Contact Report (836-314) for each consent search conducted articulating the reason for the search.
- D. Pursuant to Report Writing Manual Insert R-2, members shall complete a Stop-Data Collection Form (Scantron) for each consent search conducted.
- E. Members shall advise individuals of their right to refuse a consent search.

V. CONDUCTING STOPS

In conducting pedestrian, bicycle, or vehicle stops, members shall:

- A. be courteous, respectful, polite and professional.
- B. explain the reason for the stop while asking for identification, unless impractical.
- C. identify yourself.
- D. ensure the length of the detention is no longer than necessary to take appropriate action for the known or suspected offense, and explain the reason for any delays.
- E. answer questions the person may have regarding the stop and explain the disposition of the stop.
- F. apologize for the inconvenience when appropriate.
- G. if asked, provide the procedures for filing a complaint about police services or conduct outlined in DGO M-3 COMPLAINTS AGAINST DEPARTMENTAL PERSONNEL OR PROCEDURES.

VI. EXAMPLES OF RACIAL PROFILING

A. Examples of racial profiling include but are not limited to the following:

1. Example #1

While on patrol an officer observes a black male driving a new, expensive Mercedes Benz in a low-income neighborhood. The vehicle is not listed on the “hot sheet” nor is it entered in the Stolen Vehicle System (SVS). The officer decides to stop the vehicle to further investigate because he feels the car may be stolen because it appears too expensive for the driver and the neighborhood.

Detaining the driver of a vehicle based on the determination that a person of that race, ethnicity or national origin is unlikely to own or possess a specific model of vehicle is prohibited.

In this particular example, the officer had neither reasonable suspicion nor probable cause to detain the vehicle. Absent additional information or observations that would lead a “reasonable” officer to believe the vehicle was stolen, such as a smashed window or signs that the vehicle was hot-wired, the officer’s stop constitutes racial profiling.

2. Example #2

An officer is assigned to a predominately “white” residential neighborhood. While on patrol, the officer observes a Hispanic male driving a truck late at night. The officer knows most of the residents in the area and does not recognize the Hispanic driver. Recently there have been burglaries in that area. Based on the fact that there have been burglaries in the area, and the driver is Hispanic and the residents in the area are white, the officer stops the vehicle to further investigate.

Detaining the driver of a vehicle based on the determination a person of that race, ethnicity or national origin does not belong in a particular part of town constitutes racial profiling and is prohibited.

In this particular example, the officer’s knowledge of the residents and the driver’s race, even though the race differs from most of the residents in that area, does not provide reasonable suspicion. The

fact that there have been burglaries in the area may raise an officer's suspicion to vehicles driving late at night; however, even when this information is considered with the other factors discussed, it is an insufficient basis for a detention.

VII. STOP-DATA COLLECTION

Pursuant to Department Report Writing Manual Insert R-2, members shall:

- A. complete a Stop-Data Collection Form for every vehicle, walking, and bicycle stop conducted during their shift. Members shall also complete a Stop-Data Collection Form for every consent search conducted.
- B. print his/her name and serial number at the bottom of every Stop-Data Collection Form completed.
- C. submit completed Stop-Data Collection forms to their assigned supervisor or, in the absence of the assigned supervisor, an available field sergeant or Watch Commander for review and approval.
- D. deposit all completed (and approved) forms in the report writing receptacle at the end of their shift.

VIII. MEMBER RESPONSIBILITIES

Members shall:

- A. not engage in, ignore, or condone racial profiling or other bias-based policing.
- B. be responsible for knowing and complying with this policy.
- C. report incidents of racial profiling as defined in this policy.
- D. be subject to disciplinary action if deemed not in compliance with this order.

IX. COMPLAINTS

Complaints of racial profiling and other bias-based policing against members shall be:

- A. considered complaints of discrimination (Class 1 violation as defined in DGO M-3) and, as such, immediately forwarded to the Internal Affairs Department.
- B. immediately referred to the member's supervisor, or if the officer's supervisor is not available, to the Watch Commander.

X. TRAINING

- A. Pursuant to California Penal Code Section 13519.4, each member shall:
 - 1. attend POST racial profiling training; and
 - 2. complete an approved refresher course every five (5) years, or sooner if deemed necessary, in order to keep current with changing racial and cultural trends.
- B. The Racial Profiling Program Manager shall ensure line-up training on racial profiling and this policy is provided to sworn personnel at least once annually. This training may also be provided to non-sworn personnel.

XI. SUPERVISORY RESPONSIBILITIES

Supervisors shall:

- A. not engage in, ignore, or condone racial profiling or other bias-based policing.
- B. be responsible for knowing and complying with this policy.
- C. ensure that subordinates under their command know and understand the content and application of this policy.
- D. periodically monitor subordinates under their supervision to ensure compliance with this policy.
- E. review all forms submitted by members to ensure the forms are completed in accordance with this order and Report Writing Manual Insert R-2.

- F. print his/her name and serial number in the appropriate boxes signifying the form has been reviewed and approved, and return the form to the appropriate member.
- G. conduct periodic audits to ensure compliance with this order.

Supervisors and commanders who fail to comply with this order shall be subject to disciplinary action.

If it is determined that members assigned to a supervisor and/or commander failed to comply with this order and the supervisor and/or commander knew of said violation, or should have reasonably known, the supervisors and/or commander shall be subject to disciplinary action.

XII. BUREAU OF FIELD OPERATIONS

The Bureau of Field Operations (BFO) is responsible for data collection processing. Accordingly, BFO shall:

- A. ensure Stop-Data Collection Forms are available in the Patrol Line-up Room.
- B. enter the Stop-Data Collection Forms into the SCANTRON system within five working days of receipt.
- C. retain completed and scanned forms for period of not less than three years unless otherwise instructed by the Chief of Police.
- D. conduct periodic audits to ensure members comply with the provisions of this order and RWM Insert R-2.

XIII. OFFICE OF INSPECTOR GENERAL (OIG)

Pursuant to the provisions of DGO N-12, Departmental Audits and Inspections, the OIG shall conduct annual reviews and audits of the Department's data collection efforts to ensure compliance with the Settlement Agreement. The OIG shall report all findings to the Chief of Police and the Program Manager.

XIV. RACIAL PROFILING PROGRAM MANAGER

A. The Racial Profiling Program Manager is responsible for the following:

1. Racial profiling grant management;
2. Coordination of stop-data collection and analysis;
3. Completion of all reports pertaining to racial profiling; and
4. Coordination with the OIG to ensure compliance with the Settlement Agreement.

B. The Racial Profiling Program Manager shall:

1. produce a written report to the Chief of Police at least twice per year that includes an analysis of the data collected, and appropriate policy recommendations.
2. periodically meet with the Oakland Racial Profiling Task Force, which is comprised of representatives of the following organizations:
 - a. Oakland Police Officers' Association (OPOA);
 - b. Citizens' Police Review Board (CPRB);
 - c. American Civil Liberties Union (ACLU);
 - d. National Association for the Advancement of Colored People (NAACP); and
 - e. People United for a Better Oakland (PUEBLO).

By order of

Richard L. Word
Chief of Police

Date Signed: 26 Oct 04