CITY OF OAKLAND

Privacy Advisory Commission

April 6, 2017 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:** *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 March 27 Special Meeting Minutes.

3. 5:10pm: Open Forum
4. 5:20pm: Presentation and possible action on Request For Proposal (Crime Analysis Software) – Nicole Freeman, Oakland Police Department, Crime Analysis Manager

5. 5:50pm: Presentation and possible action on data sharing/joint operation agreements with outside entities (Oakland Police Department).

6. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

March 27, 2017 5:00 PM
Oakland City Hall
City Council Chambers
1 Frank H. Ogawa Plaza, 3rd Floor

Special 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.

Members Hofer, Brown, Katz, Oliver, and Jaquez were present.

2. 5:05pm: Review and approval of March 9 meeting minutes.

The March 9th minutes were approved by consensus.

3. 5:10pm: Open Forum

There were no open forum speakers.

4. 5:20pm: Presentation and possible action on proposed "Resolution in support of SB 31 (Lara) Religious Freedom Act" (Councilmember McElhaney).

Because CM Kalb has already submitted a resolution in support of SB31 the Commission voted to authorize the Chair to submit a letter in support of that resolution to the City Council instead of approving a separate draft resolution.

5. 5:30pm: Presentation and possible action on Surveillance Equipment Ordinance Section 8.

Chairperson Hofer provided modified language for Section 8 of the Ordinance that incorporated the same penalties for violations to the DAC, FLIR, and Cell Site Simulator technologies that exist for violations of the ordinance itself. This language was left out of Section 8, subsections 2 and 4 inadvertently. The Commission adopted these changes unanimously.

6. 5:50pm: Presentation and discussion on data sharing/joint operation agreements with outside entities (Oakland Police Department).

Deputy Chief Lois spoke about the OPD policy in regard to Immigration Customs Enforcement (ICE) and noted that a policy is being finalized and will be released very soon that clarifies OPDS's role and relationship. He emphatically stated that the current policy already precludes officers from participating in any form of immigration enforcement but that in light of recent events and Oakland's stance as a sanctuary city, it was important to revise and make the policy more specific.

Captain Holmgren and Lt. Wehrly also were present to discuss the Safe Streets program and how they interct with the FBI, the U.S. Marshalls and the ATF. Concerns were raised about information OPD shares with ARIES that could then be shared with ICE and therefore OPD could inadvertently be providing info to ICE. DC Lois noted that because Oakland does not collect information on people's immigration status, there is no info for ICE to gather.

Questions arose about the Safe Streets MOU with the FBI and its focus on Overtime costs but it was determined that the full MOU with the FBI was not included in the packet and will be included in the next agenda packet as it is far more thorough at defining each agency's role.

No action was taken and the item was continued to the April meeting.

7. 7:00pm: Adjournment.

The meeting adjourned at 6:30pm.

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Document Overview

The primary purpose of this document is to create a framework for collecting the information necessary to make an informed recommendation regarding contemplated surveillance technology equipment and their use. In addition, this document is intended to instill consistency, objectivity, and transparency in the assessment process. It is expected that this framework will be augmented and improved with each evaluation of surveillance technology by the Privacy Advisory Commission (PAC).

Pursuant to the Surveillance Equipment Ordinance, a City entity or department seeking approval of such equipment acquisition or use shall complete this Surveillance Technology Assessment Questionnaire (STAQ), and incorporate the information into the required Surveillance Impact Report (SIR) pertaining to the acquisition or use. All categories may not be applicable to every technology. The table below provides a cross reference between the SIR and STAQ to facilitate completion of the SIR by the City entities.

SIR Section	STAQ Section
a. Description	1. Technology Solution Overview
b. Purpose	1. Technology Solution Overview
c. Location	4. Location(s) of Deployment and Data Storage
d. Impact	5. Protecting Civil Rights and Liberties
e. Data Sources	2. Surveillance Technology Detail
f. Data Security	3. Authorized Users
g. Fiscal Cost	6. Initial and On-going Costs of Technology
h. Third Party Dependence	2. Surveillance Technology Detail
i. Alternatives	1. Technology Solution Overview
j. Track Record	1. Technology Solution Overview

Questionnaire

Question		Response	Supporting Documentation
1		**Why: Technology Solution Overview**	
1.1	What is the function of the technology as described by the manufacturer?	Provide crime analysts with various technology tools to represent existing crime data	
1.2	What is the specific problem this equipment or use will resolve?	Mapping and investigative technology	
1.3	How will success be demonstrated?	Efficient products not currently available to aid tactical, administrative, and strategic police	
1.4	What is the success rate		

January 5, 2017

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

	Question	Response	Supporting Documentation
	for this equipment or use?		
1.5	What non-surveillance alternatives were considered?	This is not a surveillance RFP	
1.6	Why were the non-surveillance alternatives not pursued?	This is not a surveillance RFP	
2	**What: Surveillance Technology Detail**		
2.1	What equipment capabilities do you intend to use?	Data management and processing	
2.2	What other equipment capabilities are possible?		
2.3	What safeguards will be implemented to ensure that unauthorized capabilities or uses will not be implemented?	Technology tools will only be available to authorized and credentialed users at OPD. Vendors must adhere to all secureity and CJIS-compliant standards regarding data storage and management	
2.4	What information can the technology capture?	Information from OPD CAD and LRMS databases	
2.5	What information can the technology store?	Information from the OPD CAD and LRMS databases	
2.6	How long will information be retained?	As long as the data is stored in OPD CAD and LRMS databases	
2.7	Will the data gathered and stored by handled by a third party on an on-going basis	yes	
2.8	How will you ensure that data is not retained for longer than allowed?	Vendors must adhere to all secureity and CJIS-compliant standards regarding data sortage and management	
3	**Who: Authorized Users**		
3.1	Who is authorized to access the technology?	Technology tools will only be available to authorized and credentialed users at OPD.	
3.2	How are users authenticated?	Must be OPD employees (all OPD employees must undergoe full background and mandatory DoJ training on confidentiality of police data.	
3.3	How is access to the technology audited?	Will be determined once products are selected	
3.4	What is the mechanism for monitoring compliance with access	Will be determined once products are selected	

Question		Response	Supporting Documentation
	policies?		
4		**Where: Location(s) of deployment and data storage**	
4.1	Where will the technology be deployed within the community?	Nowhere – these are internal products	
4.2	What is the basis for selecting these locations?	N/A	
4.3	What are the crime statistics for each proposed deployment location?		
4.4	Where will the information be stored (on-site, remote, cloud)?	On-site and remotely -- Vendors must adhere to all secureity and CJIS-compliant standards regarding data storage and management	
4.5	What are the safeguards, monitors, and audits to ensure security of information at storage (at rest) and when accessed (transmission)?	Will be determined once products are selected	
5		**How: Protecting Civil Rights and Liberties**	
5.1	Could the technology or use collect information related to race, citizenship status, gender, age, socioeconomic level, reproductive choices, or sexual orientation? If so, what safeguards are in place to limit such collection?	All authorised users must be OPD employees (all OPD employees must undergoe full background and mandatory DoJ training on confidentiality of police data.	
5.2	Will the technology be deployed in communities with minority residents, non-citizens, low-income residents, or any group historically vulnerable to disproportionate civil liberties violations?	These are internal products; products that store intelligence information must be 28CFR23 compliant	
5.3	Could the technology be used on groups, public	These are internal products; products that store intelligence information must be 28CFR23	

Question	Response	Supporting Documentation
gatherings, or crowds and thus have an effect on First Amendment activities such as protests? If so, what safeguards are in place to limit this?		
5.4 Does the technology collect and retain information about individuals not suspected of wrongdoing? If so, how could such information impact their right to privacy?	These are internal products; products that store intelligence information must be 28CFR23 compliant	
6	**How Much: Initial and On-going Costs of Technology**	
6.1 What are the initial costs, including acquisition, infrastructure upgrades, licensing, software, training, and hiring of personnel?	Will be determined once products are selected	
6.2 What are the ongoing costs, including measures to secure data and data storage?	Will be determined once products are selected	
6.3 What is the funding source for the proposed acquisition or use?	Will be determined once products are selected	
6.4 Are there other tools capable of furthering the identified purpose that the community may wish to spend these funds on (e.g., community-based policing, improved lighting)?	No	