CITY OF OAKLAND

AGENDA REPORT

TO: Sabrina B. Landreth
City Administrator

FROM: Joe DeVries
Asst. to the City Administrator

SUBJECT: Creation of a Privacy Advisory Commission

DATE: October 14, 2015

City Administrator Approval Date: 12/3/15

RECOMMENDATION

Staff Recommends That The City Council Adopt An Ordinance Establishing The Privacy Advisory Commission, Providing For The Appointment Of Members Thereof, And Defining The Duties And Functions Of Said Commission.

EXECUTIVE SUMMARY

Approval of this ordinance will create a nine-member Oakland Privacy Advisory Commission with members appointed by the Mayor and approved by the City Council, as set forth in the City Charter.

BACKGROUND / LEGISLATIVE HISTORY

On March 4, 2014 the City Council passed Resolution No.84869 C.M.S. ***(Attachment A)*** which stated in part, "that a Data Retention and Privacy Policy shall be developed by a Council-approved advisory body prior to the activation of the Port-only Domain Awareness Center (DAC), and members of said body will be appointed by each member of the City Council." This led to the creation of an Ad Hoc Privacy and Data Retention Policy Advisory Committee (Advisory Committee) to establish a Privacy and Data Retention Policy for the Port Domain Awareness Center (the Policy).

The Advisory Committee met for over a year and developed the Policy which was adopted as Resolution No.85638 C.M.S. on June 2, 2015 ***(Attachment B).*** Section II. A. of the Resolution states that "The City Council shall establish a citywide Permanent Privacy Policy Advisory Committee. The Permanent Privacy Policy Advisory Committee shall have jurisdiction as determined by the City Council, including but not limited to reviewing and advising on any proposed changes to this Policy or to the DAC."

Item: _____
Public Safety Committee
December 15, 2015

The Advisory Committee also made several additional recommendations to the City Council including a recommendation that this newly formed committee be empowered to develop a Surveillance Technology Ordinance that would create a public process to determine future surveillance technology purchases and allowable uses. At the June 2, 2015 meeting the City Council voted in favor of this recommendation and directed staff to return in the fall with an Ordinance establishing a Permanent Privacy Advisory Committee with the development of such an Ordinance as the committee's initial work.

On April 21, 2015, the City Council adopted Resolution No.85532 C.M.S. ***(Attachment C)*** which authorized the City Administrator to enter into an agreement with the U.S. Department of Homeland Security for Fiscal Year (FY) 2015 for the purchase and ongoing maintenance of a Law Enforcement Air Unit Forward Looking Infrared Thermal Imaging Camera System (FLIR) to allow for situational awareness and air patrol for the City and Port of Oakland.

Due to concerns regarding the need for a policy governing the use of the FLIR, the resolution also called for the City's DAC Advisory Committee to draft and present a Privacy and Data Retention Policy for the FLIR. The Advisory Committee was selected for this task since it was already actively meeting around the DAC Policy and no other such advisory body existed.

The Advisory Committee held two meetings to discuss and develop the FLIR Policy including a discussion with Oakland Police Department (OPD) Personnel. The Advisory Committee produced a draft Policy that Council adopted on October 6, 2015 as Resolution No.85807 C.M.S. ***(Attachment D)*** The FLIR Policy was modeled after the DAC Policy and the speed with which it was developed by the Advisory Committee demonstrated how effective an existing advisory body can be at developing policy surrounding the use of surveillance technology that is effective at protecting civil liberties while not hampering emergency responders' ability to conduct their work.

ANALYSIS AND POLICY ALTERNATIVES

The proposed Privacy Advisory Commission will consist of nine (9) members, at least six (6) of whom are Oakland residents, appointed by the Mayor and approved by the City Council, as set forth in the City Charter. To assure that terms overlap, appointments shall be as follows: three (3) initial members will serve a three-year initial term, three (3) initial members will serve two-year initial term, and the other three (3) initial members will serve a one-year initial term.

Members will include a balance of experienced professionals with backgrounds in civil rights/defense, law enforcement, computer hardware, software or encryption, accounting/auditing, and general members of the public that have demonstrated an interest in privacy rights.

Specifically, members of the Privacy Commission will represent the following criteria, with no more than two (2) members representing any one criteria and at least one from each criteria to the extent possible:

1. an attorney, legal scholar, or activist with expertise in privacy, civil rights, or a representative of an organization with expertise in the same such as but not limited to the American Civil Liberties Union, the Electronic Frontier Foundation, and the National Lawyers Guild;

2. a past or present member of member of law enforcement who has worked with surveillance equipment and other technology that collects or stores citizen data;

3. an auditor or certified public accountant;

4. a hardware, software, or encryption security professional

5. A member of an organization which focuses on government transparency and openness such as but not limited to the League of Women Voters or Open Oakland or an individual such as a former government employee with experience working on government transparency and openness.

Council Resolution Nos.85638 C.M.S. and 85807 C.M.S. specify that the Privacy Advisory Commission will have jurisdiction as determined by the City Council, to review and advise on any proposed changes to the DAC Policy, the FLIR Policy, or to the DAC itself. All changes proposed to the Policies or to the DAC must be submitted to, reviewed, and evaluated by the Privacy Advisory Commission for recommendation for submission to the City Council, and include an opportunity for public meetings, a public comment period of no fewer than 30 days, and written agency response to these comments.

Beyond these specific duties, the Council also supported the staff recommendation in June that the Privacy Advisory Commission should be charged with drafting a Surveillance Technology Ordinance for Council consideration. Such an ordinance would create a public process whereby residents and interested parties would have the opportunity to express their concern about new technology that enhances surveillance capabilities or otherwise has the potential to impact residents' privacy or civil liberties before the City enters into any contractual or grant agreements to purchase such technology. Upon adoption of an ordinance, the Privacy Advisory Commission could be charged with conducting those hearings on the City Council's behalf related to the proposed technologies, and then providing a recommendation as to how the City should proceed. Similar to the DAC and FLIR Policies, the Commission could also be charged with developing Privacy Policies for any future surveillance technologies that the City decides to purchase. The Commission will also be able to advise the City on its use, storage, and protection of data.

The Commission would be charged with making yearly reports and recommendations to the City Council regarding the City's use of surveillance equipment, and any proposed or existing surveillance equipment privacy and data retention policies. Finally, the Commission can provide an analysis of pending federal, state or local legislation that may affect privacy, as defined in this ordinance, in Oakland or for Oakland residents.

FISCAL IMPACT

Staff anticipates that the Commission will require about 10-15 staff hours per month to support a monthly meeting of the Privacy Advisory Commission. This support would include: assisting the chairperson in preparing the meeting agenda, developing and distributing the meeting agenda packet and supporting materials, posting meeting notices in accordance with the Brown Act and Sunshine Ordinance, responding to informational requests from Commission members and coordinating subject matter experts and other City staff to appear on relevant agenda topics. This time would be absorbed by existing staff, so there is no additional cost implication. However, after the initial implementation phase and depending on the breadth of items such as a surveillance technology ordinance, the staff time required could be such that additional resources would need to be identified to meet the needs of the Commission.

PUBLIC OUTREACH/INTEREST

The ordinance to create a permanent Privacy Advisory Commission was first proposed by the DAC Advisory Committee and received overwhelming support in on-line engagement forums, at the Advisory Committee meetings, and during multiple discussions at the Public safety Committee.

COORDINATION

This report was reviewed by the Oakland Police Department, the Office of the City Clerk, the Controller's Bureau, and the Office of the City Attorney.

SUSTAINABLE OPPORTUNITIES

***Economic**: This information presented in this report presents no economic impact.*

***Environmental**: There are no environmental opportunities identified in this report.*

***Social Equity**: The creation of a Privacy Advisory Commission provides residents with an indication that the City responds appropriately to concerns about civil liberties and privacy during a time of rapidly evolving technology. By establishing safeguards to prevent potential abuse of technology, the City strengthens residents' faith in local government and allows for robust public dialogue and increased trust.*

For questions regarding this report, please contact Joe DeVries, Assistant to the City Administrator at (510) 238-3083.

Respectfully submitted,

Joe DeVries
Assistant to the City Administrator
City Administrator's Office

Reviewed by:

Amadis Sotelo
Deputy City Attorney

Attachment A- Resolution No. 84869 C.M.S.
Attachment B- Resolution No. 85638 C.M.S.
Attachment C- Resolution No. 85532 C.M.S.
Attachment D- Resolution No. 85807 C.M.S.

Attachment A

Approved as to Form and Legality

City Attorney

REVISED AT CITY COUNCIL MEETING ON MARCH 4, 2014

OAKLAND CITY COUNCIL

RESOLUTION NO. 84869 C.M.S.

Introduced by Councilmember _____

RESOLUTION AUTHORIZING THE CITY ADMINISTRATOR TO NEGOTIATE AND EXECUTE A PROFESSIONAL SERVICES AGREEMENT WITH SCHNEIDER ELECTRIC INC. TO PROVIDE PROFESSIONAL SERVICES FOR DESIGN/BUILD/MAINTAIN SERVICES REPRESENTED IN PHASE 2 OF THE CITY AND PORT JOINT DOMAIN AWARENESS CENTER (DAC) PROJECT FOR AN AMOUNT NOT TO EXCEED $1,600,000

WHEREAS, Congress and the Obama Administration intended the Port Security Grant Program (PSGP) to be one of the tools in a comprehensive set of measures to strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks; and

WHEREAS, the Port of Oakland submitted PSGP grant proposals to jointly develop, establish and operate a City/Port Domain Awareness Center (DAC) utilizing the City of Oakland Emergency Operations Center (EOC) to consolidate a network of existing surveillance and security sensor data to actively monitor critical Port facilities, utility infrastructure, City facilities and roadways; and

WHEREAS, on May 23, 2013, the Port of Oakland Board of Directors approved a resolution for the Port of Oakland to enter into a Memorandum of Understanding and Grant Administration Agreement to provide up to two million dollars ($2,000,000) of supplemental FY09 and FY10 PSGP grant funding with the City of Oakland to further expand the development of the City/Port Domain Awareness Center (DAC) and embark upon Phase 2 of the expansion of the systems integration as well as equipment/system enhancements; and

WHEREAS, on July 30, 2013, the City Council passed Resolution No. 84593, approving the appropriation of grant funds required agreements between the City and the Port, and

WHEREAS, on November 19, 2013, the City Council pursuant to Resolution 84725, waived further advertising and the competitive Request For Proposals selection requirements of the Oakland Municipal Code, and authorized the staff to select a vendor from the pool of vendors that responded to the RFP titled, "City of Oakland/Port of Oakland Joint Domain Awareness Center, October 2012" in an amount not to exceed $2 million dollars, and

WHEREAS, the City seeks to utilize these additional funds to complete Phase 2 of the Domain Awareness Center (Phase 2); and

WHEREAS, the City wishes to negotiate a new contract for Phase 2 work, which consists of, but is not limited to, additional enhancements to the Emergency Operations Center, additional systems' integration such as the Port Geographic Information Systems (GIS) and other key City Public Safety Information Technology systems, and

WHEREAS, the City finds and determines that the services provided pursuant to the agreement authorized hereunder are of a professional, scientific or technical nature and are temporary in nature; and

WHEREAS, the City finds and determines that this contract shall not result in the loss of employment or salary by any person having permanent status in the competitive service; now, therefore, be it

RESOLVED: that the City Administrator or her designee is authorized to accept, appropriate, and administer up to two million dollars ($2,000,000) of American Recovery and Reinvestment Act (ARRA) supplemental Port Security Grant funds for (PSGP) fiscal years 2009 and 2010 for Phase 2 of the joint Port of Oakland/City Domain Awareness Center (DAC) project; and be it

FURTHER RESOLVED: That the City Administrator or her designee is hereby authorized to execute a Professional Services Contract with Schneider Electric, Inc. in an amount not to exceed $1,6000,000 million dollars to provide design/build/maintenance services for Phase 2 of the City and Port of Oakland joint Domain Awareness Center (DAC) project, for an amount not to exceed One million six hundred thousand dollars ($1,600,000), pending a determination of its full compliance with applicable laws, including the Nuclear Free Zone Act; and be it

FURTHER RESOLVED: That The Domain Awareness Center will only be implemented in a Port-only approach and shall hereafter be referred to as the "Port Domain Awareness Center" (DAC); and be it

FURTHER RESOLVED: That the following items will be removed from DAC Phase I Integration: (a) Shot Spotter in areas outside of the immediate Port Area, and (b) 40 City Traffic Cameras identified on pages 9 and 10 of the City Administrator's Supplemental Agenda report accompanying this Resolution; and be it

FURTHER RESOLVED: That the following items will be removed from DAC Phase II Integration: (a) Police and Fire Records Management Systems (RMS), and (b) any news feeds and alerts except those expressly listed in the City Administrator's Supplemental Agenda report accompanying this Resolution; and be it

FURTHER RESOLVED: That staff shall: (1) develop a clear definition of the Police and Fire Computer Aided Dispatch (CAD) that will be integrated into the DAC, and (2) develop a protocol for the use of such CAD data by the DAC; and be it

FURTHER RESOLVED: That operation of any DAC program beyond the Port area may only move forward upon explicit approval of the Council; and be it

FURTHER RESOLVED: That City, as opposed to Port Area, Shot Spotter is specifically excluded from the Port-only Domain Awareness Center program and may only be included in the future upon approval of Council; and be it

FURTHER RESOLVED: That there will be no data or information sharing with any local, state or federal agency/entity without a written Memorandum of Understanding that has been approved by the Council; and be it

FURTHER RESOLVED: That no new systems or capabilities can be added to the DAC without express City Council approval, including, but not limited to, technological functionalities such as facial recognition, other forms of analytics (like "gait analysis," in which someone can be identified based on the way they walk) or other capabilities that haven't yet been invented but are soon to come; and be it

FURTHER RESOLVED: That work-flow plans and a budget for the same shall be developed prior to the activation of the Port-only Domain Awareness Center; and be it

FURTHER RESOLVED: That the contract with Schneider Electric, Inc. shall include the DAC program policies and requirements set forth in all of the foregoing Resolved and Further Resolved paragraphs; and be it

FURTHER RESOLVED: That a "Data Retention" and a "Privacy Policy" shall be developed by a Council-approved advisory body prior to the activation of the Port-only Domain Awareness Center, and members of said advisory body will be appointed by each member of the City Council; and be it

FURTHER RESOLVED: That Staff will return to the Council with a status report on the project in three (3) months; and be it

FURTHER RESOLVED: That approval of this contract is contingent on inclusion in the Phase 2 contract of a liquidated damages provision should the contract be unable to meet grant deadlines as well as an indemnification clause should the contractor be found in violation of Oakland's Nuclear Free Zone Ordinance; and be it

FURTHER RESOLVED: That this Resolution does not commit any operational funding for the DAC at this time, but to the extent that staff brings any requests for funding in the future such requests shall include an a fair-share contribution option from the Port of Oakland as well as an option with no additional City staffing.

FURTHER RESOLVED: That funds to complete this project will be drawn from Fund (2123), Org (20711), Program (PS21), Accounts and Projects to be Determined; and be it.

FURTHER RESOLVED: That the City Administrator or her designee is authorized to accept and appropriate said FY 2009 and FY2010 PSGP Grants funds into U.S. Department of Homeland Security Fund (2123), Emergency Management Services Division (20711) a grant project to be determined, and Emergency Management Service Program (PS21), the full grant

funds will be appropriated to the Miscellaneous Federal Grants Accounts (46129); and be it

FURTHER RESOLVED: That the agreement(s) and other actions authorized hereunder shall be reviewed and approved by the Office of the City Attorney for form and legality and filed with the Office of the City Clerk, and shall comply with previous resolutions regarding this particular project's successful adoption of a privacy and data retention policy as a condition of project implementation.

IN COUNCIL, OAKLAND, CALIFORNIA, MAR 4 2014

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, ~~GALLO~~, ~~KAPLAN~~, KALB, ~~GIBSON MCELHANEY~~, REID, ~~SCHAAF~~ and PRESIDENT KERNIGHAN – 5 Quan

NOES – Gallo, Gibson McElhaney, Kaplan, Schaaf – 4

ABSENT – 0

ABSTENTION – 0

ATTEST: LaTonda Simmons

LaTonda Simmons
City Clerk and Clerk of the Council
of the City of Oakland, California

Attachment B

Approved as to Form and Legality

City Attorney

As Amended By City Council on June 2, 2015

OAKLAND CITY COUNCIL

RESOLUTION NO. 85638 C.M.S.

Introduced by Councilmember _____

RESOLUTION (1) ESTABLISHING THE CITY OF OAKLAND'S POLICY FOR PRIVACY AND DATA RETENTION FOR THE PORT DOMAIN AWARENESS CENTER (DAC) AND (2) CONSIDERATION FOR FUTURE ACTION OF AN ORDINANCE IMPOSING ENFORCEMENT PENALTIES INCLUDING CREATING A PRIVATE RIGHT OF ACTION TO SEEK A WRIT OF MANDATE, INJUNCTIVE AND/OR DECLARATORY RELIEF

I. BACKGROUND AND OVERVIEW

WHEREAS, the Port Domain Awareness Center (interchangeably referred to in this document as the "Port Domain Awareness Center," "Domain Awareness Center," or "DAC") was first proposed to the City Council's Public Safety Committee on June 18, 2009, in an informational report regarding the City of Oakland partnering with the Port of Oakland to apply for Port Security Grant funding under the American Recovery and Reinvestment Act of 2009; and

WHEREAS, under this grant program, funding was available for Maritime Domain Awareness (MDA) projects relative to "maritime" or "waterside" uses. The Port and City were encouraged to consider the development of a joint City-Port Domain Awareness Center. The joint DAC could create a center that would bring together the technology, systems, and processes that would provide for an effective understanding of anything associated with the City of Oakland boundaries as well as the Oakland maritime operations that could impact the security, safety, economy, or environment. However, the City Council action on March 4th, 2014 limited the scope of the DAC to the Port. Any effort to expand the DAC beyond the Port would require a public hearing and action by the City Council; and

WHEREAS, "Port Domain Awareness" is defined as the effective understanding of anything associated with all areas and things of, on, under, relating to, adjacent to, or bordering the e sea, ocean, or other navigable waterways, including all first responder and maritime related activities, infrastructure, people, cargo, and vessels and other conveyances that could impact the security, safety, economy, or environment; and

WHEREAS, the DAC would be used as a tool or system to accomplish this effective understanding as it relates to the security, safety, economy, or environment of the Port of Oakland; and

WHEREAS, the DAC is a joint project between the Port and the City of Oakland. The DAC is physically located within the Emergency Operations Center (EOC) and it can collect and monitor live streams of video, audio, and/or data, watching for time-critical events that require an immediate response. Additionally, the DAC is the part of the EOC that stays alert between emergencies and refers Port-adjacent incidents to the EOC staff for the EOC activation decision. While the rest of the EOC activates, the DAC can share relevant information to incident participants until the EOC infrastructure takes over. Notwithstanding any other provision to the contrary, this Policy applies only to the City-Port DAC systems operated by the City of Oakland's Emergency Operations Center in Oakland, California which are under the City's control, and does not apply to Port of Oakland monitoring and security systems operated by the Port and which are outside the City's jurisdiction or control; and

WHEREAS, the mission of the DAC is to have situational awareness needed for time-critical decision making in order to prevent, prepare for, respond to, and recover from emergencies and crime at the Port; and

WHEREAS, this policy's purpose is to protect the Right to Privacy, civil liberties, and freedom of speech of the general public as protected by the California and Federal Constitutions, and erect safeguards around any data captured and retained by the DAC, and to protect against its improper use, distribution, and/or breach and in how it is used for law enforcement investigations. This policy shall be referred to as the DAC Privacy and Data Retention Policy ("Policy"). More specifically, the principal intent of this Policy is to ensure the DAC adheres to constitutionality, especially the 1st and 4th amendments of the U.S. Constitution and the California Constitution. Also, this Policy is designed to see that the DAC processes are transparent, presume people's innocence, and protect all people's privacy and civil liberties; and

WHEREAS, privacy includes our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, associations, secrets, and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose. The importance of privacy can be illustrated by dividing privacy into three equally significant parts: 1) Secrecy - our ability to keep our opinions known only to those we intend to receive them, without secrecy, people may not discuss affairs with whom they choose, excluding those with whom they do not wish to converse. 2) Anonymity - Secrecy about who is sending and receiving an opinion or message, and 3) Autonomy - Ability to make our own life decisions free from any force that has violated our secrecy or anonymity; and

WHEREAS, this Policy is designed to promote a "presumption of privacy" which simply means that individuals do not relinquish their right to privacy when they leave private spaces and that as a general rule people do not expect or desire for law enforcement to monitor, record, and/or aggregate their activities without cause or as a consequence of participating in modern society; and

WHEREAS, in adopting this Policy, it is not the intent of the City Council to supersede or suspend the functions, duties, and authority of the City to manage and oversee the affairs of the

City and to protect public safety. This Policy is intended to affirm the rights of privacy and freedom of expression, in conformance with and consistent with federal and state law. Nothing in this Policy shall be interpreted as relieving the City's responsibility to comply with any and all labor and union agreements, and to comply with all other City Council applicable policies; and

WHEREAS, for any policy provision that imposes a criminal penalty and/or creates a private right of action to be enforceable, Council must first pass an ordinance providing for such remedies; and prior to Council adopting such an ordinance, the City must meet and confer with the affected employee unions; now therefore be it

RESOLVED: That any updates to the policy and to DAC will be subject to the following:

II. DAC POLICY DEVELOPMENTS AND UPDATES

A. The City Council shall establish a citywide Permanent ~~Privacy Policy Advisory Committee for the DAC~~ Privacy Policy Advisory Committee. The Permanent Privacy Policy Advisory Committee shall have jurisdiction as determined by the City Council, including but not limited to reviewing and advising on any proposed changes to this Policy or to the DAC. Further, this Policy must be reviewed by the Permanent Privacy Policy Advisory Committee at least once a year.

B. No changes to this Policy shall occur without City Council approval. This Policy is developed as a working document, and will be periodically updated to ensure the relevance of the Policy with the ever changing field of technology. All changes proposed to the Policy or to the DAC must be submitted to and reviewed and evaluated by the permanent Privacy Policy Advisory Committee for recommendation for submission to the City Council, and include an opportunity for public meetings, a public comment period of no fewer than 30 days, and written agency response to these comments. City Council approval shall not occur until after the 30 day public comment period and written agency response period has completed.

C. For any proposed changes for the Policy that occur prior to the City Council establishing the permanent Privacy Policy Advisory Committee, such changes shall be in the purview of the City Council.

D. The requirements and limitations for the DAC required by City Council Resolution 84869 of March 4, 2014, are incorporated herein by reference, as follows:

1. That the Domain Awareness Center will only be implemented in a Port-only approach a[nd] shall hereafter be referred to as the "Port Domain Awareness Center (DAC);

2. That the following items will be removed from the DAC Phase I integration: (a) Shot Spotter in immediate areas outside of the Port Area, and (b) 40 City Traffic Cameras identified on pages 9 and 10 of the City Administrator's Supplemental Agenda Report, dated February 27, 2014;

3. That the following items will be removed from DAC Phase II integration: (a) Police and Fire Records Management Systems (RMS), and (b) any news feeds and alerts except those expressly listed in the City Administrator's Supplemental Agenda Report, dated February 27, 2014,

4. That staff shall: (1) develop a clear definition of the Police and Fire Computer Aided Dispatch (CAD) that will be integrated into the DAC, and (2) develop a protocol for the use of such CAD data by the DAC,

5. That operation of any DAC program beyond the Port area may only move forward upon explicit approval of the Council,

6. That City, as opposed to Port, Shot Spotter is specifically excluded from the Port-only Domain Awareness Center program and may only be included in the future upon approval by the Council,

7. That there will be no data or information sharing with any local, state, or federal agency/entity without a written Memorandum of Understanding that has been approved by Council; and be it

8. That no new system capabilities can be added to the DAC without express City Council approval, including, but not limited to technological functionalities such as facial recognition, other forms of analytics (like "gait analysis", in which someone can be identified based on the way they walk) or other capabilities that haven't yet been invented but are soon to come; and be it

FURTHER RESOLVED: That the following definitions apply to this policy:

III. DEFINITIONS

"Allowable Use" means the list of uses allowable for the DAC as specified below in this policy;

"Analytics" means the discovery and understanding of meaningful patterns and trends in data for well-informed decisions. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance;

"Bookmark" means a feature of the Physical Security Information Management (PSIM) system that allows staff to mark and annotate data for later review; the time stamped record is the bookmark;

"ITD" means the City of Oakland's Information Technology Department;

"DAC Application" means the VIDSYS Software;

"DAC Data" means any data or information fed into, stored, collected, or captured by the DAC System, or derived therefrom;

"DAC Staff" refers to the specific City of Oakland employees who as part of their regular duties are responsible for using the DAC System, including supervisors, and ~~that~~ have completed appropriate training prior to interaction with the DAC;

"DAC System" means access and use of the following combined feeds and systems in one application: Port Security Cameras (Phase 1), Port Intrusion Detection System (IDS) (Phase 1), Port Geographic Information System (GIS) (Phase 2), Port Vessel Tracking (Phase 2), Port Truck Management (Phase 2), Police and Fire CAD (Phase 2), WebEOC Notifications (Phase 2), Tsunami Alerts (Phase 2), Police and Fire Automatic Vehicle Location (Phase 2), National Oceanic and Atmospheric Administration (NOAA) Weather Alerts (Phase 2), United States Geological Survey (USGS) Earthquake Information (Phase 2), City of Oakland Shot Spotter Audio Sensor System (only those sensors that provide coverage to Port areas), and the physical security information system, server, attached storage, and mobile devices. "DAC System" does not refer to the use of any of these systems or feeds outside the DAC Application;

"DAC Vendors" means the various vendors who support and maintain the DAC computer and network equipment;

"EOC" means Oakland's Emergency Operations Center, a facility and service of the Oakland Fire Department's Emergency Management Services Division (EMSD). The EMSD ensures "that the City of Oakland and community are at the highest level of readiness and able to prevent, mitigate against, prepare for, respond to and recover from the effects of natural and human-caused emergencies that threaten lives, property and the environment." "EMSD also supports the coordination of the response efforts of Oakland's Police, Fire and other first responders in the City's state-of-the-art Emergency Operations Center to ensure maximum results for responders, the ability to provide up-to-date public information and the ability to provide the best resource management during a crisis. Additionally, EMSD coordinates with the Operational Area and other partner agencies to guarantee the seamless integration of federal, state and private resources into local response and recovery operations. The EOC is a secure facility with access limited to City employees with a need for access, contractors, and security-cleared members of partner organizations. The EOC facility hosts the joint City-Port DAC systems, data, and staff."

"Major Emergency" means the existence of conditions of disaster or extreme peril to the safety of persons and property within the territorial limits of the Port of Oakland or having a significant adverse impact within the territorial limits of the Port of Oakland, caused by such conditions as air pollution, fire, flood, storm, epidemic, drought, sudden and severe energy shortage, plant or animal infestation or disease, the state Governor's warning of an earthquake or volcanic prediction, an earthquake, or other conditions, which are likely to be beyond the control

of the services, personnel, equipment, and facilities of the City of Oakland and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requiring extraordinary measures beyond the authority vested in the California Public Utilities Commission.

"Need To Know" means even if one has all the necessary official approvals (such as a security clearance) to access the DAC System, one shall not be given access to the system or DAC Data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the Allowable Uses in Section VIII A. of this Policy. Furthermore, the "need" shall be established prior to access being granted by the designated City official or their designee and shall be recorded in accordance with Internal Recordkeeping requirements under Section IX.

"Personally Identifiable Information" ("PII") means any data or information that alone or together with other information can be tied to an individual with reasonable certainty. This includes, but is not limited to one's name, social security number, physical description, home address, telephone number, other telephone identifiers, education, financial matters, medical history, employment history, photographs of faces, whereabouts, distinguishing marks, license plates, cellphone meta-data, and internet connection meta-data.

"Protected Activity" means all rights including without limitation: speech, associations, conduct, and privacy rights including but not limited to expression, advocacy, association, or participation in expressive conduct to further any political or social opinion or religious belief as protected by the United States Constitution and/or the California Constitution and/or applicable statutes and regulations. The First Amendment does not permit government "to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *White v. Lee* (9th Cir. 2000) 227 F.3d 1214, 1227; *Brandenburg v. Ohio* (1969) 395 U.S. 444, 447.

> **Example of speech <u>not</u> protected by 1st Amendment:** *People v. Rubin* (1979) 96 C.A.3d 968. Defendant Rubin, a national director of the Jewish Defense League, held a press conference in California to protest a planned demonstration by the American Nazi Party to take place in Illinois in five weeks. During his remarks, Rubin stated: "We are offering five hundred dollars . . . to any member of the community . . . who kills, maims, or seriously injures a member of the American Nazi Party. . . . This is not said in jest, we are deadly serious." Rubin was charged with solicitation for murder. The appeals court upheld the charge, reasoning that Rubin's words were sufficiently imminent and likely to produce action on the part of those who heard him. *Id.* at 978-979.
>
> **Example of speech protected by 1st Amendment:** *Watts v. U.S.* (1969) 394 U.S. 705. The defendant, Watts, stated that he would refuse induction into the armed forces and "if they ever make me carry a rifle the first man I want in my sights is L.B.J." and was federally charged with "knowingly and willfully threatening the president." The Court reasoned that Watts did not make a "true 'threat'" but instead was merely engaging in a

type of political hyperbole. Id., at 708.

For purposes of determining whether sufficient grounds exist for any of the allowable DAC uses authorized under this policy under the Section "Allowable uses", "Reasonable Suspicion" means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise. Reasonable Suspicion shall not be based on Protected Activity. A suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

The "Right to Privacy" is recognized by the California Constitution as follows:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. Cal. Const. Art. 1, Section 1; and be it

FURTHER RESOLVED: That access to the DAC system and equipment shall be as follows:

IV. ACCESS TO THE DAC SYSTEM / EQUIPMENT

A. Day to Day Operations

The DAC computer and network equipment is maintained by the DAC Staff and DAC Vendors. Only DAC Staff as defined by this policy will be authorized to monitor DAC Data in the regular course of business. ~~Employees assigned to monitor DAC Data are required to undergo security background checks at the local level as well as security clearances required at state and federal levels.~~ These employees will be required to sign binding Non-Disclosure Agreements to ensure data and information security.

B. Training

Training by the Chief Privacy Officer is required prior to interaction with the DAC System. All DAC Staff who are assigned to monitor the DAC Data will be required to participate in specific training around constitutional rights, protections, and appropriate uses of the DAC System and consequences for violating this Policy.

C. Critical incidents/emergencies/EOC activations

During an Allowable Use as defined by this policy, and notwithstanding the requirements in Access to Information and Data Section, City of Oakland officials and officers such as the City Administrator, Mayor, City Council Members, City Attorney, Department Directors and/or their designees , and outside governmental and non-governmental agencies assisting with the Allowable Use (such as the Red Cross) and who report to EOC, may have limited access to live

data from the DAC System only on a Need To Know basis and if there was a direct correlation between the Allowable Use and DAC operations. Nothing in this policy shall be construed to conflict with the duties and responsibilities of City of Oakland officers and officials under the Oakland City Charter, Articles I through V.

D. Support and Repairs

ITD staff and DAC Vendors that installed the systems will have access to the DAC System components but will only have access to DAC Data for the purpose of carrying out their job functions. Various manufacturers and vendors are hired to provide additional support services. Any system and network level access by DAC Vendors requires a background check. The system level access is maintained by ITD staff, however the Applications level access, as far as end-users are concerned, is maintained by the DAC Staff.

E. Funding Auditing Purposes

Federal, State, or Local funding auditors may have access to only equipment, hardware, and software solely for audit purposes and must abide by the requirements of this Policy; and be it

FURTHER RESOLVED: That access to information and data obtained through the DAC shall be as follows:

V. ACCESS TO INFORMATION AND DATA OBTAINED THROUGH DAC

A. **Access:** Access to DAC Data shall be limited exclusively to City and Port employees with a Need To Know. Other than DAC Staff, any sworn or non-sworn personnel without a direct role in investigating, auditing, or responding to an incident will not be permitted access to DAC Data.

B. **Data Sharing**: If the DAC Data that is being requested is from an outside feeder source, the law enforcement agency seeking such information must go to the original source of the information to request the data, video or information. In order for DAC Staff to provide DAC Data to non-City of Oakland agencies there must be a warrant based upon probable cause, court order, or a written Memorandum of Understanding (MOU) or Contract approved by the City Council after enactment of this Policy. Any legislation authorizing such MOU or Contract must clearly state whether the MOU or Contract will allow for DAC Data to be shared with another agency. Furthermore, any such MOU or Contract must provide in the title of such document that it authorizes the sharing of DAC Data with another agency.

C. **Retention:** The DAC shall not record any data except bookmarks of Allowable Uses as defined below ~~in Section VIII~~; and be it

FURTHER RESOLVED: That the allowable uses for the DAC data/system shall be as follows:

VI. ALLOWABLE USES

A. **Uses**: The following situations at the Port are the only ones in which the use of the DAC is allowable and may be activated in response to:

Active Shooter
Aircraft Accident or Fire
Barricaded Subject
Bomb/Explosion
Bomb Threat
Burglary
Cargo Train Derailment
Chemical or Biological Incident
Container Theft
Earthquake
Electrical Substation Intruder Alarm
Fire
Flooding-Water Main Break
HAZMAT Incident
Hostage Situation
Major Emergency
Marine Terminal Fence Line Intruder Alarm
Mass Casualty Incident
Major Acts of Violence (likely to cause great bodily injury)
Medical Emergency
Missing or Abducted Person
Pandemic Disease
Passenger Train Derailment
Person Overboard
Port Terminal/Warehouse Intruder
Power Outage
Radiation/Nuclear Event Detected
Severe Storm
Ship Accident or Fire
Ship Intruder/Breach
Supply Chain Disruption
Street Racing/Side Show
Takeover of a vehicle or vessel (transit jack)
Telecommunications/Radio Failure
Transportation Worker Identification Credential (TWIC) Access Control Violation
Tsunami Warning
Technical Rescue
Unauthorized Person in Secure Zone
Unmanned Aerial Vehicle in Port airspace
Vehicle Accident requiring emergency medical attention
Wildfire -3 Alarm or greater

B. The DAC shall not be used to infringe, monitor, or intrude upon Protected Activity except where all of the following conditions are met:

1. There is a Reasonable Suspicion of criminal wrongdoing; and

2. DAC Staff articulates the facts and circumstances surrounding the use and basis for Reasonable Suspicion in a written statement filed with the Chief Privacy Officer no later than 8 hours after activation of the DAC System; and be it

FURTHER RESOLVED: That the following internal controls, audits and reporting metrics shall apply to the DAC data:

VII. INTERNAL CONTROLS, AUDITS AND REPORTING METRICS

A. Chief Privacy Officer

"Chief Privacy Officer" (CPO) refers to the City Administrator or a senior level employee designated by the City Administrator who is responsible for managing the risks and business impacts of privacy laws and policies. The CPO will determine that procedure manuals, checklists, and other directives used by staff are kept up-to-date and consistent with policies and procedures related to privacy for the DAC functions, City measures, or other legislative measures related to privacy issues. The CPO will also oversee any training required to maintain compliance.

B. Internal Controls

Controls should be designed to ensure appropriate access and use of the data related to DAC activities and to prevent and/or detect unauthorized access or use.

C. Compliance Officer

The Compliance Officer is an employee whose responsibilities include ensuring that the organization complies with internal policies and outside regulatory requirements. The Compliance Officer will be responsible for establishing the operational controls and procedures necessary for assessing compliance, including but not limited to the following standard operating procedures and practices.

D. Internal Recordkeeping

DAC Staff shall keep the enumerated records in this section for a period of no less than two years to support compliance with this Policy and allow for independent third party auditors to readily search and understand the DAC System and DAC Data. The records shall include, but not be limited to, the below enumerated categories:

1. A written list of methods for storing bookmarks and DAC Data, including how the data is to be secured, segregated, labeled, or indexed;
2. A written list of who may access the DAC System and DAC Data and persons responsible for authorizing such access; and
3. Auditing mechanisms that track and record how the DAC System and DAC Data are viewed, accessed, shared, analyzed, modified, bookmarked, deleted, or

retained. For each such action, the logs shall include timestamps, the person who performed such action, and a justification for it (e.g., specific authorized use).

4. DAC System Usage: An overview of how the DAC System is used including:
   a. Listing and number of incident records by incident category
   b. Timing required to close an incident record
   c. Actionable events, non-actionable events, and false alarms.

5. Public Safety Effectiveness: Summary, general information, and evaluations about whether the DAC is meeting its stated purpose, to include a review and assessment of:
   d. Crime statistics for geographic areas where the DAC was used;
   e. The frequency in which DAC was used to bookmark or retain data for potential criminal investigations;
   f. The occurrences in which DAC Data was shared for potential criminal investigations;
   g. Lives saved;
   h. Incidents in which assistance was provided to persons, property, land and Natural Habitat security,

6. Data Sharing: A summary of how the DAC data is shared with other non-City entities, to include a review and assessment of:
   i. The type of data disclosed;
   j. Justification for disclosure (e.g., warrant, memoranda of understanding, etc.)
   k. The recipient of the data;
   l. Dates and times of disclosure; and
   m. Obligations imposed on the recipient of shared information.

7. Data Minimization: A reporting of the incidents, if any, of disclosure of DAC Data that do not comply with the Policy, follow-up procedures, resolutions and consequences.
8. Protected Activity Exception: A reporting of the incidents, if any, of the use of the Protected Activity Exception waiver, as provided in Section VIII B, copies of written certifications, follow-up procedures, resolutions, and consequences.
9. Dispute Resolution: A summary and description of the number and nature of complaints filed by citizens or whistleblowers and the resolution of each, as required or permitted by the City's Whistleblower program.
10. Requests for Change: A summary of all requests made to the City Council for approval of the acquisition of additional equipment, software, data, or personnel services, relevant to the functions and uses of the DAC and the pertinent data, including whether the City approved or rejected the proposal and/or required changes to this Policy before approval.
11. Data Retention: A summary of the data retained within the DAC Application and an assessment of compliance to the Data Retention requirements as stated in the Policy.
12. System Access Rights Audit: The process to provide access and specific permission levels to authorized persons/staff working in the DAC function.
13. Public Access: A summary of the public records requests received, responses, and an evaluation of the appropriateness of records submitted and timeliness of responses.

14. Cost: Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs; and be it

FURTHER RESOLVED: That the following internal control reviews and audits shall apply to the DAC data/system:

VIII. INTERNAL CONTROL REVIEWS AND AUDITS

A. Internal Control Reviews

The Compliance Officer will perform regular self-assessments (internal control reviews) of the DAC's Internal Controls and will summarize the findings and remediation plans, if any, and report these to the City Administrator and City Auditor and be made publicly available to the extent the release of such information is not prohibited by law.

B. Audits

The City Auditor will consider the function of the DAC and the relevant risks to the private data retained to determine the scope and frequency of performance audits to be conducted by the City Auditor.

Quarterly and as needed audits of the DAC System will be conducted and made publicly available to the extent the release of such information is not prohibited by law, by the Compliance Officer to ensure compliance with this Policy. The audit shall include the following information and describe any corrective action taken or needed:

C. Annual Report

The Compliance Officer shall prepare and present an Annual Report that summarizes and includes the results of Internal Recordkeeping, Internal Control Self-Assessments, and Independent Audits to the extent the release of such information is not prohibited by law, and present it to the appropriate Committee of the City Council or to the City Council at a public meeting at a designated timing each year. The City Council should use the Report and the information it is based on to publically reassess whether the DAC benefits outweigh the fiscal and civil liberties costs; and be it

FURTHER RESOLVED: That the following records management protocols shall apply to the DAC data/system as follows:

IX. RECORDS MANAGEMENT

A. The DAC Staff will be the custodian of records; responsible for retention, access to information, and responding to requests for information under California's Public Records Act.

B. DAC Staff must comply with all relevant and applicable Data Retention policies and procedures, regulations and laws; and be it

X. PUBLIC INFORMATION REQUESTS

FURTHER RESOLVED: That to the extent the release of such information is not prohibited by law, all protocols, public records, including but not limited to use logs, audits, DAC Data, and any sharing agreement, shall be available to the public upon request; and be it

XI. SANCTIONS AND ENFORCEMENT REMEDIES

FURTHER RESOLVED: That violations of this Policy shall result in consequences that may include retraining, suspension, termination, and if applicable, criminal fines and penalties, or individual civil liability and attorney's fees and/or damages as provided by law, depending on the severity of the violation; and be it

XII. SEVERABILITY

FURTHER RESOLVED: That if any section, subsection, sentence, clause or phrase of this Policy is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Policy. The City Council hereby declares that it would have adopted this Policy and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

JUN 02 2015

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL WASHINGTON, GALLO, GUILLEN, KALB, KAPLAN, REID, and PRESIDENT GIBSON MCELHANEY – 7

NOES - 0

ABSENT - Kaplan - 1

ABSTENTION - 0

ATTEST: LaTonda Simmons

LaTonda Simmons
City Clerk and Clerk of the Council
of the City of Oakland, California

Attachment C

Approved as to Form and Legality

City Attorney

FILED
OFFICE OF THE CITY CLERK
OAKLAND

15 APR 23 PM 2:01

REVISED IN CITY COUNCIL APRIL 21, 2015

OAKLAND CITY COUNCIL

RESOLUTION NO. 85532 C.M.S.

RESOLUTION:

1) AUTHORIZING THE CITY ADMINISTRATOR OR HIS DESIGNEE TO:

A. ENTER INTO AN AGREEMENT WITH THE U.S. DEPARTMENT OF HOMELAND SECURITY FOR FISCAL YEAR 2014/2015 PORT SECURITY GRANT PROGRAM (PSGP) FUNDS IN AN AMOUNT UP TO FIVE HUNDRED SEVENTY-EIGHT THOUSAND, FIVE HUNDRED AND TWENTY-SEVEN DOLLARS ($578,527); AND

B. ACCEPT, APPROPRIATE, AND ADMINISTER SAID FUNDS; AND

C. APPROVE THE PRELIMINARY SPENDING PLAN WHICH INCLUDES THE PURCHASE OF A VIDEO SECURITY SYSTEM FOR THE EMERGENCY OPERATIONS CENTER (EOC) AND THE FIRE DISPATCH CENTER (FDC) AND THE PURCHASE OF A LAW ENFORCEMENT AIR UNIT FLIR FOR THE CITY AND PORT OF OAKLAND; ~~AND SPECIFICALLY, THE FIRE DEPARTMENT'S PURCHASE OF A VIDEO SECURITY SYSTEM FOR THE EMERGENCY OPERATIONS CENTER (EOC);~~ AND

D. EXPEND FUNDS IN ACCORDANCE WITH THE PRELIMINARY SPENDING PLAN INCLUDING PURCHASES OF EQUIPMENT AND SERVICES IN EXCESS OF THE CITY ADMINISTRATOR'S PURCHASING AUTHORITY; AND

E. AUTHORIZE THE USE OF EXISTING (BUDGETED) FUNDING IN THE AMOUNT OF ONE HUNDRED NINETY-TWO THOUSAND, EIGHT HUNDRED AND FORTY TWO DOLLARS ($192,842) FROM GENERAL PURPOSE FUND FOR PERSONNEL AND OTHER ADMINISTRATIVE RESOURCES, TO SATISFY THE IN-KIND MATCH REQUIREMENT; AND

2) WAIVING THE CITY OF OAKLAND'S ADVERTISING AND BIDDING REQUIREMENTS FOR ITEMS REQUIRED TO BE PURCHASED FROM THE FEDERALLY AUTHORIZED EQUIPMENT LIST ("AEL")

WHEREAS, the U.S. Department of Homeland Security's Fiscal Year (FY) 2014/2015 Port Security Grant Program (PSGP) allocates grant funds to address ports considered of the highest risk status to assist ports in enhancing risk management capabilities and support a strategic, area-wide focus around ports providing funding for the development and implementation of port-wide risk management and mitigation activities, as well as continuity of operations by building capacity to prevent, protect against, respond to, and recover from acts of terrorism and terrorist threats against the Port; and

WHEREAS, the City of Oakland Port Security Grant Program ("PSGP") grant proposal was approved and the City of Oakland has been awarded a FY 2014/15 PSGP grant allocation of five hundred seventy-eight thousand, five hundred and twenty-seventy dollars ($578,527) by the U.S. Department of Homeland Security; and

WHEREAS, the U.S. Department of Homeland Security awarded the City of Oakland $578,527 in grant funds for the federal Fiscal Year 2014/15 to fund the Oakland Fire Department, Emergency Management Services Division for the grant performance period of September 1, 2014 through August 31, 2016; and

WHEREAS, the grant designates the amount not to exceed $578,527 be expended for the purchase of specified equipment, supplies and contracted services identified on the Federally Authorized Equipment List ("AEL"); and

WHEREAS, the City of Oakland Port Security Grant Program ("PSGP") requires a match of in-kind/cash in an amount not to exceed one hundred ninety-two thousand, eight hundred and forty-two dollars ($192,842); and

WHEREAS, the Oakland Police Department and the Oakland Fire Department will provide an in-kind match of up to one hundred ninety-two thousand, eight hundred and forty-two dollars ($192,842) from General Purpose Fund for personnel and other administrative resources, to satisfy the in-kind/cash match requirement; and

~~**WHEREAS, this resolution does not provide authority for the purchase of the Law Enforcement Air Unit FLIR; and**~~

WHEREAS, the Oakland Fire Department, Office of Emergency Management Services Division and Homeland Security staff are also essential in managing and coordinating the FY 2014/15 PSGP which provides for $28,927 or 5% funding for maintenance and administration of the total grant award; and

WHEREAS, the City of Oakland is committed to cooperating with our regional partners to detect, prevent, prepare for, respond to and recover from acts of terrorisms and threats of terrorism and effectively carry out the program of the FY 2014/15 PSGP grant; and

WHEREAS, the Oakland Municipal Code Section 2.04.030.A requires Council approval for any purchase of goods and/or services over $100,000; and

WHEREAS, the City Administrator recommends that he or his designee be authorized to expend Fiscal Year 2014/15 Port Security Grant Program (PSGP) U.S. Department of Homeland Security grant funds for this grant in excess of $100,000 and up to $578,527; and

WHEREAS, funds will be appropriated to the Homeland Security Fund (2123), the Emergency Management Services Division Organization (20711), Emergency Management Services Program (PS 21) and project number to be determined; and

WHEREAS, the City Administrator has determined that any services that may be provided under contracts authorized hereunder would be of a professional, scientific or technical and temporary nature and not result in the loss of employment or salary by any person having permanent status in the competitive service; and

WHEREAS, Oakland Municipal Code section 2.04.050.I.5 permits the Council to waive the advertising and bidding requirements upon a finding that it is in the best interest of the City to do so; and

WHEREAS, staff recommends that it is in the best interests of the city to waive advertising and bidding processes for items required by the grant terms to be purchased from the federally authorized equipment list ("AEL"); now, therefore be it

RESOLVED: That the City Administrator or his designee is authorized to enter into a grant agreement with the U.S. Department of Homeland Security to accept funds in an amount up to five hundred seventy-eight thousand, five hundred and twenty-seven dollars ($578,527) from the Port Security Grant Program (PSGP); and be it

FURTHER RESOLVED: That the City Administrator or his designee is authorized to accept, appropriate and administer said funds; and be it

FURTHER RESOLVED: That funds will be appropriated to the Homeland Security Fund (2123), the Emergency Management Services Division Organization (20711), Emergency Management Services Program (PS 21) and project number to be determined; and be it

FURTHER RESOLVED: That the City Administrator or his designee is authorized to approve the 2014/15 PSGP preliminary spending plan and that the spending plan includes the purchase of the Emergency Operations Center (EOC) and Fire Dispatch Center (FDC) Camera Security System ~~for the Fire Department, Emergency Management Services Division and the purchase of the Law Enforcement Air Unit FLIR for the City and Port of Oakland~~ and the purchase of the Law Enforcement Air Unit FLIR for the City and Port of Oakland; and be it

FURTHER RESOLVED: That the City Administrator or his designee is authorized make all purchases of goods, material, equipment, services or combination thereof identified in the approved 2014/15 PSGP preliminary spending plan, including equipment on the Federal Authorized Equipment List (AEL) and services required by the grant, including purchases that exceed the City Administrator's purchasing authority under Oakland Municipal Code section 2.04.20; and be it

FURTHER RESOLVED: That the Council finds that pursuant to Oakland Municipal Code section 2.04.050.I.5, for the reason stated above and in the City Administrator's report accompanying this resolution, that it is in the best interest of the City to waive the advertising and bidding requirements for items to be purchased pursuant to grant terms that require such purchase(s) be made from the federally authorized equipment list ("AEL") and so waives such requirements; and be it

FURTHER RESOLVED: That the City Administrator or his designee is authorized to expend from existing appropriation of one hundred ninety-two thousand, eight hundred and forty-two dollars $192,842 from General Purpose Fund 1010.20711.Project To Be Determined (TBD) and 1010.107410. Project To Be Determined (TBD) for personnel and other administrative resources, to satisfy the in-kind/cash match requirement; and be it

FURTHER RESOLVED: That the 2014/15 Port Security Grant Program (PSGP) grant allocation funds received by the City of Oakland may only ~~only~~ be used specifically for project #1 ~~project #1~~ the purchase and allowable maintenance costs of the EOC and FDC Camera Security System; and for project #2, the purchase and allowable maintenance costs of the Law Enforcement Air Unit FLIR Camera that allows for Situational Awareness and Air patrol for the City and Port of Oakland;~~and for project #2, the purchase and allowable maintenance costs of the Law Enforcement Air Unit FLIR Camera that allows for Situational Awareness and Air portal for the City and Port of Oakland~~ and be it

FURTHER RESOLVED: That no information processed by the Law Enforcement Air Unit FLIR Camera will be collected, retained, stored, or disseminated by the Oakland Police Department and the Oakland Fire Department in their use of the Law Enforcement Air Unit FLIR Camera; and be it

FURTHER RESOLVED: That the DAC Ad Hoc Committee shall, before the City Council's 2015 summer recess, draft and present a Privacy and Data Retention Policy that specifies the allowable uses of, and governs the collection, retention, storage, and dissemination of information processed by, the Law Enforcement Air Unit FLIR Camera; and be it

FURTHER RESOLVED: That the prohibition on dissemination of information does not include the prohibition of the Oakland Police Department from communicating critical information obtained through the use of the FLIR, such as a fleeing suspect's location, to outside agencies assisting in the immediate apprehension of a fleeing suspect who is not inside a private residence; and be it

FURTHER RESOLVED: That staff will return to council for contract authority for purchasing 2014/15 PSGP funded equipment not specified in this resolution~~, such as the Law Enforcement Air Unit FLIR;~~ and be it

FURTHER RESOLVED: That the 2014/15 PSGP grant allocation received by the City of Oakland may not be used for the purchase of any aerial drones, stingray, or facial recognition technology or facial recognition software; and be it

FURTHER RESOLVED: That ongoing costs, such as maintenance for equipment or goods purchased with 2014/15 PSGP grant will be absorbed in each of the respective City of Oakland agencies' existing budget with no additional General Purpose fund appropriations; and be it
FURTHER RESOLVED: That the City Administrator or his designee is authorized to approve the preliminary spending plan; and be it

FURTHER RESOLVED: That all contracts authorized hereunder shall be approved for form and legality by the Office of the City Attorney and placed on file in the Office of the City Clerk.

IN COUNCIL, OAKLAND, CALIFORNIA, APR 21 2015, 20_____

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL WASHINGTON, GALLO, GUILLEN, KALB, [redacted], [redacted], and PRESIDENT GIBSON MCELHANEY – 6

NOES- Ø

ABSENT- Ø

ABSTENTION- Kaplan - 1

– Excused - Reid - 1

ATTEST: LaTonda Simmons

LaTonda Simmons
City Clerk and Clerk of the
Council of the City of Oakland,

California

Attachment B

Approved as to Form and Legality

City Attorney

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2015 SEP 24 PM 1:01

AMENDED AT PUBLIC SAFETY COMMITTEE ON SEPTEMBER 15, 2015

OAKLAND CITY COUNCIL

RESOLUTION NO. 85807 C.M.S.

Introduced by Councilmember _____

RESOLUTION ESTABLISHING THE CITY OF OAKLAND'S FORWARD LOOKING INFRARED THERMAL IMAGING CAMERA SYSTEM (FLIR) PRIVACY AND DATA RETENTION POLICY WHICH PRESCRIBES THE RULES FOR THE USE OF THE FLIR; ESTABLISHES OVERSIGHT, AUDITING AND REPORTING REQUIREMENTS; AND IDENTIFIES PENALTIES FOR VIOLATIONS

I. BACKGROUND AND OVERVIEW

WHEREAS, the Law Enforcement Forward Looking Infrared Thermal Imaging Camera System ("FLIR") was first proposed to the City Council's Public Safety Committee on March 24, 2015. The purchase of the FLIR will be funded by Federal FY 2014/15 Port Security Grant Program ("PSGP") monies. The Oakland City Council approved acceptance of the PSGP funds and authorized purchase of the FLIR on April 21, 2015; and

WHEREAS, a thermal imaging camera is a device that forms an image using infrared radiation, similar to a common camera that forms an image using visible light. FLIR technology is commonly used by law enforcement or firefighters when visibility is poor, such as at night, or when smoke is present; and

WHEREAS, in *Kyllo v. United States*, the United States Supreme Court ruled directly on thermal imaging systems, holding that law enforcement must first obtain a warrant when using a FLIR to search a private residence; and

WHEREAS, the Court in *Kyollo* stated: "[w]here, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant." *Kyllo v. US*, (2001) 533 U.S. 27; and

II. POLICY PURPOSE

WHEREAS, this policy's purpose is to protect the Right to Privacy, civil liberties, and freedom of speech of the general public as protected by the California and Federal Constitutions, and erect safeguards around any data captured and retained by the FLIR, and to protect against its improper use, distribution, and/or breach and in how it is used for law enforcement investigations. This policy shall be referred to as the FLIR Privacy and Data Retention Policy ("Policy"). More specifically, the principal intent of this Policy is to ensure that FLIR use adheres to

constitutionality, especially the 1st and 4th amendments of the U.S. Constitution, and the California Constitution's Article 1. Also, this Policy is designed to see that the FLIR processes are transparent, presume people's innocence, and protect all people's privacy and civil liberties; and

WHEREAS, privacy includes our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, associations, secrets, and identity. The Right to Privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose. The importance of privacy can be illustrated by dividing privacy into three equally significant parts: 1) Secrecy - our ability to keep our opinions known only to those we intend to receive them, without secrecy, people may not discuss affairs with whom they choose, excluding those with whom they do not wish to converse. 2) Anonymity - Secrecy about who is sending and receiving an opinion or message, and 3) Autonomy - Ability to make our own life decisions free from any force that has violated our secrecy or anonymity; and

WHEREAS, this policy is designed to promote a "presumption of privacy" which simply means that individuals do not relinquish their Right to Privacy when they leave private spaces and that as a general rule people do not expect or desire for law enforcement to monitor, record, and/or aggregate their activities without cause or as a consequence of participating in modern society; and

WHEREAS, in adopting this policy, it is not the intent of the City Council to supersede or suspend the functions, duties, and authority of the City to manage and oversee the affairs of the City and to protect public safety. This Policy is intended to affirm the Right to Privacy and freedom of expression, in conformance with and consistent with federal and state law. Nothing in this Policy shall be interpreted as relieving the City's responsibility to comply with any and all labor and union agreements, and to comply with all other City Council applicable policies; ~~and~~

~~**WHEREAS,** for any policy provision that imposes a criminal penalty, creates a private right of action, and/or allows for injunctive relief to be enforceable, Council must first pass an ordinance providing for such remedies; and prior to Council adopting such an ordinance, the City must meet and confer with the affected employee unions;~~ now therefore be it

RESOLVED: That any updates to the policy and to FLIR will be subject to the following:

III. FLIR POLICY DEVELOPMENTS AND UPDATES

A. The City Council shall establish a citywide Permanent Privacy Policy Advisory Committee. The City's Permanent Privacy Policy Advisory Committee shall have jurisdiction as determined by the City Council, including but not limited to reviewing and advising on any proposed changes to this Policy or to the FLIR's technical capabilities or use

B. No changes to this Policy shall occur without City Council approval. This Policy is developed as a working document, and will be periodically updated to ensure the relevance of this Policy with the ever changing field of technology. All changes proposed to this Policy must be submitted to and reviewed and evaluated by the Permanent Privacy Policy Advisory

Committee for recommendation for submission to the City Council, and include an opportunity for public meetings, a public comment period of no fewer than 30 days, and written agency response to these comments. City Council approval shall not occur until after the 30 day public comment period and written agency response period has completed.

C. For any proposed changes for the Policy that occur prior to the City Council establishing the permanent Privacy Policy Advisory Committee, such changes shall be in the purview of the City Council.

D. The requirements and limitations for the FLIR required by City Council Resolution No. 85532 on April 21, 2015, are incorporated herein by reference, as follows:

1: That no information processed by the Law Enforcement Air Unit FLIR Camera will be collected, retained, stored, or disseminated by the Oakland Police Department and the Oakland Fire Department in their use of the Law Enforcement Air Unit FLIR Camera; and be it

2: That the DAC Ad Hoc Committee shall, before the City Council's 2015 summer recess, draft and present a Privacy and Data Retention Policy that specifies the allowable uses of and governs the collection, retention, storage, and dissemination of information processed by the Law Enforcement Air Unit FLIR Camera; and be it

3: That the prohibition on dissemination of information does not include the prohibition of the Oakland Police Department from communicating critical information obtained through the use of the FLIR such as a fleeing suspect's location, to outside agencies assisting in the immediate apprehension of a fleeing suspect who is not inside a private residence;

FURTHER RESOLVED: That the following definitions apply to this policy:

III. DEFINITIONS

"Allowable Use" means the list of uses in Section VI A. of this Policy for which the FLIR can be used.

"FLIR" means a thermal imaging camera that forms an image using infrared radiation, similar to a common camera that forms an image using visible light.

"FLIR Data" means any data, images, or information fed into, stored, collected, or captured by the FLIR, or derived therefrom.

"FLIR Staff" means the City of Oakland police and fire department employees who will be responsible for using the FLIR, including supervisors, and that have completed appropriate training prior to interaction with the FLIR.

"FLIR Vendors" means the various vendors who support and maintain the FLIR.

"ITD" means the City of Oakland's Information Technology Department.

"Need To Know" means even if one has all the necessary official approvals (such as a security clearance) to access the FLIR, one shall not be given access to the FLIR or FLIR Data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the Allowable Uses in Section VIII A. of this Policy. Furthermore, the "need" shall be established prior to access being granted by the designated City official or their designee and shall be recorded in accordance with Internal Recordkeeping requirements under Section IX.

"Personally Identifiable Information" ("PII") means any data or information that alone or together with other information can be tied to an individual with reasonable certainty. This includes, but is not limited to one's name, social security number, physical description, home address, telephone number, other telephone identifiers, education, financial matters, medical history, employment history, photographs of faces, whereabouts, distinguishing marks, license plates, gait, cellphone meta-data, and internet connection meta-data.

"Protected Activity" means all rights including without limitation: speech, associations, conduct, and privacy rights including but not limited to expression, advocacy, association, or participation in expressive conduct to further any political or social opinion or religious belief as protected by the United States Constitution and/or the California Constitution and/or applicable statutes and regulations. The First Amendment does not permit government "to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *White v. Lee* (9th Cir. 2000) 227 F.3d 1214, 1227; *Brandenburg v. Ohio* (1969) 395 U.S. 444, 447.

> **Example of speech <u>not</u> protected by 1st Amendment:** *People v. Rubin* (1979) 96 C.A.3d 968. Defendant Rubin, a national director of the Jewish Defense League, held a press conference in California to protest a planned demonstration by the American Nazi Party to take place in Illinois in five weeks. During his remarks, Rubin stated: "We are offering five hundred dollars . . . to any member of the community . . . who kills, maims, or seriously injures a member of the American Nazi Party. . . . This is not said in jest, we are deadly serious." Rubin was charged with solicitation for murder. The appeals court upheld the charge, reasoning that Rubin's words were sufficiently imminent and likely to produce action on the part of those who heard him. *Id.* at 978-979.
>
> **Example of speech protected by 1st Amendment:** *Watts v. U.S.* (1969) 394 U.S. 705. The defendant, Watts, stated that he would refuse induction into the armed forces and "if they ever make me carry a rifle the first man I want in my sights is L.B.J." and was federally charged with "knowingly and willfully threatening the president." The Court, reasoned that Watts did not make a "true 'threat'" but instead was merely engaging in a type of political hyperbole. Id., at 708.

"Reasonable Suspicion" means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise.

Reasonable Suspicion shall not be based on Protected Activity. Furthermore, a suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

"Right to Privacy" is recognized by the California Constitution as follows:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. Cal. Const. Art. 1, Section 1.

FURTHER RESOLVED: That access to the FLIR system and equipment shall be as follows:

IV. ACCESS TO THE FLIR EQUIPMENT

A. Day to Day Operations

The FLIR is maintained by the FLIR Staff and FLIR Vendors. Only FLIR Staff will be used to monitor incoming FLIR Data.

B. Training

Training by the Chief Privacy Officer is required prior to interaction with the FLIR. All FLIR Staff who are assigned to monitor the FLIR Data will be required to participate in specific training around constitutional rights, protections, and appropriate uses of the FLIR and consequences for violating this Policy.

C. Support and Repairs

City staff and FLIR Vendors that installed the FLIR will have access to the FLIR but may only have access to FLIR Data for the purpose of carrying out their job functions. Any FLIR access by FLIR Vendors requires a background check.

D. Funding Auditing Purposes

Federal, State, or Local funding auditors may have access to only equipment, hardware, and software solely for audit purposes and must abide by the requirements of this Policy.

FURTHER RESOLVED: That access to information and data obtained through the FLIR shall be as follows:

V. ~~ACCESS TO~~ USE OF INFORMATION AND DATA OBTAINED THROUGH FLIR

A. **Access:** Access to the incoming FLIR Data shall be limited exclusively to City employees and elected officials with a Need To Know. Other than FLIR Staff, any sworn or non-sworn

personnel without a direct role in investigating, auditing, or responding to an incident will not be permitted access to the incoming FLIR Data.

B. **Data Sharing:** The above restriction on access to FLIR Data in Section VI.A does not prohibit the Oakland Police Department from communicating critical information obtained or derived from the FLIR Data, such as a fleeing suspect's location, to outside agencies assisting in the immediate apprehension of a fleeing suspect who is not inside a private residence.

C. **Prohibition on Data Retention:** The FLIR shall not collect (other than real-time), retain, store, or disseminate any data.

FURTHER RESOLVED: That the allowable uses for the FLIR data/system shall be as follows:

VI. ALLOWABLE USES

A. **Uses**: The following situations are the only ones in which use of the FLIR is allowable and may be activated in response to:

Active Shooter
Aircraft accident or fire
Barricaded subject
Firefighting investigation, suppression, or firefighter support
Facilitating search and rescue efforts over land or water
Hot pursuit of suspect
Locating vehicles or aircraft in remote areas
Missing/abducted person
Special Events, as defined by the Oakland Municipal Code, which occur in public places

B. The FLIR shall not be used to infringe or intrude upon Protected Activity except where all of the following conditions are met:

1) There is a Reasonable Suspicion of criminal wrongdoing; and

2) FLIR Staff articulates the facts and circumstances surrounding the use and basis for Reasonable Suspicion in a written statement filed with the Chief Privacy Officer no later than 8 hours after use of the FLIR.

FURTHER RESOLVED: That the following internal controls, audits and reporting metrics shall apply to the FLIR data:

VII. INTERNAL CONTROLS, AUDITS AND REPORTING METRICS

A. Chief Privacy Officer

Chief Privacy Officer (CPO) refers to the City Administrator or a senior level employee designated by the City Administrator who is responsible for managing the risks and business impacts of privacy laws and policies. The CPO will determine that procedure manuals, checklists, and other directives used by staff are kept up-to-date and consistent with policies and

procedures related to privacy for the FLIR functions, City measures, or other legislative measures related to privacy issues. The CPO will also oversee any training required to maintain compliance.

B. Internal Controls

Controls should be designed to ensure appropriate access and use of the data related to FLIR activities and to prevent and/or detect unauthorized access or use.

C. Compliance Officer

The Compliance Officer is an employee, designated by the City Administrator, whose responsibilities include ensuring that functions related to the FLIR comply with the Policy, other relevant City policies, and regulatory requirements. In doing so, the Compliance Officer will design operational controls that relate but are not limited to the below areas within the FLIR function. These operational controls shall be presented to the Permanent Privacy Policy Committee annually and upon update.

D. Internal Recordkeeping

FLIR Staff shall keep the enumerated records in this section for a period of no less than two years to support compliance with this Policy and allow for independent third party auditors to readily search and understand the FLIR and FLIR Data. The records shall include, but not be limited to, the below enumerated categories:

1. A written list of who may access the FLIR and FLIR Data and person(s) responsible for authorizing such access.
2. Auditing mechanisms that track and record how the FLIR is accessed and FLIR Data viewed, accessed, shared, analyzed, and deleted. For each such action, the logs shall include timestamps, the person who performed such action, and a justification for it (e.g., specific authorized use, maintenance).
3. **FLIR Usage**: An overview of how the FLIR is used including:
    a. Listing and number of incident records by incident category
    b. Timing required to close an incident record
    c. Actionable events, non-actionable events, and false alarms.
4. **Public Safety Effectiveness:** Summary, general information, and evaluations about whether the FLIR is meeting its stated purpose, to include a review and assessment of:
    a. Crime statistics for geographic areas where the FLIR was used;
    b. The occurrences in which information derived from FLIR Data was used for potential criminal investigations;
    c. Lives saved;
    d. Incidents in which assistance was provided to persons, property, land and Natural Habitat security.
5. **Information Sharing:** A summary of how information derived from FLIR Data is shared with other non-City entities, to include a review and assessment of:
    a. The type of information disclosed;
    b. Justification for disclosure (e.g., warrant, real-time mutual assistance, etc.)

c. The recipient of the information;
d. Dates and times of disclosure; and
e. Obligations imposed on the recipient of shared information.

6. **Data Minimization:** A reporting of the incidents, if any, of improper access or disclosure of FLIR Data that do not comply with the Policy, including follow-up procedures, resolutions and consequences.
7. **Protected Activity Exception:** A reporting of the incidents, if any, of the use of the Protected Activity Exception waiver, as provided in Section VI B, including copies of written certifications, follow-up procedures, resolutions, and consequences.
8. **Dispute Resolution:** A summary and description of the number and nature of complaints filed by citizens or whistleblowers and the resolution of each, unless prohibited by law or the City's Whistleblower program.
9. **Requests for Change**: A summary of all requests made to the City Council for approval of the acquisition of additional equipment, software, data, technical capabilities or features, or personnel services, relevant to the functions and uses of the FLIR and the pertinent data, including whether the City approved or rejected the proposal and/or required changes to this Policy before approval.
10. **Data Retention:** An assessment of compliance with the Data Retention prohibition as stated in the Policy.
11. **System Access Rights Audit**: The process to provide access and specific permission levels to authorized persons/staff working with the FLIR.
12. **Public Access:** A summary of the public records requests received, responses, and an evaluation of the appropriateness of records submitted and timeliness of responses.
13. **Cost:** Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs.

FURTHER RESOLVED: That the following internal control reviews and audits shall apply to the FLIR data/system:

VIII. INTERNAL CONTROL REVIEWS AND AUDITS

A. Internal Control Reviews

The Compliance Officer will perform regular self-assessments (internal control reviews) of the FLIR's Internal Controls and will summarize the findings and remediation plans, if any, and report these to the City Administrator and City Auditor and be made publicly available to the extent the release of such information is not prohibited by law.

B. Audits

The City Auditor will consider the function of the FLIR and the relevant risks to privacy and all civil liberties to determine the scope and frequency of performance audits to be conducted by the City Auditor.

Quarterly and as needed audits of the FLIR will be conducted and made publicly available to the extent the release of such information is not prohibited by law, by the Compliance Officer to

ensure compliance with this Policy. The audit shall include the following information and describe any corrective action taken or needed:

C. Annual Report

The Compliance Officer shall prepare and present an Annual Report that summarizes and includes the results of Internal Recordkeeping, Internal Control Self-Assessments, and Independent Audits to the extent the release of such information is not prohibited by law, and present it to the appropriate Committee of the City Council or to the City Council at a public meeting at a designated timing each year. The City Council should use the Report and the information it is based on to publically reassess whether the FLIR benefits outweigh the fiscal and civil liberties costs.

FURTHER RESOLVED: That the following records management protocols shall apply to the FLIR data/system as follows:

IX. RECORDS MANAGEMENT

A. The FLIR Staff will be the custodian of records; responsible for retention (as noted in Section VII), access to information, and responding to requests for information under California's Public Records Act.

B. FLIR Staff must comply with all relevant and applicable Data Retention policies and procedures, regulations and laws; and be it

X. PUBLIC INFORMATION REQUESTS

FURTHER RESOLVED: That to the extent the release of such information is not prohibited by law, all protocols and public records, including but not limited to use logs, and audits, shall be available to the public upon request; and be it

XI. SANCTIONS AND ENFORCEMENT REMEDIES

FURTHER RESOLVED: That violations of this Policy shall result in consequences that may include retraining, suspension, termination, and if applicable, criminal fines and penalties, or individual civil liability and attorney's fees and/or damages as provided by California or Oakland law, depending on the severity of the violation; and be it

XII. SEVERABILITY

FURTHER RESOLVED: That if any section, subsection, sentence, clause or phrase of this Policy is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Policy. The City Council hereby declares that it would have adopted this Policy and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

IN COUNCIL, OAKLAND, CALIFORNIA, OCT 06 2015

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL WASHINGTON, GALLO, GUILLEN, KALB, KAPLAN, REID, and PRESIDENT GIBSON MCELHANEY — 8

NOES - Ø

ABSENT - Ø

ABSTENTION - Ø

ATTEST: LaTonda Simmons

LaTonda Simmons
City Clerk and Clerk of the Council
of the City of Oakland, California

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2015 DEC -3 PM 5:56

APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

INTRODUCED BY COUNCILMEMBER _____

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

ORDINANCE ESTABLISHING THE PRIVACY ADVISORY COMMISSION, PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, AND DEFINING THE DUTIES AND FUNCTIONS OF SAID COMMISSION

WHEREAS, on June 2, 2015, City Council approved, in concept, the creation of a standing community advisory board on privacy issues, and further requested that City Administration prepare an ordinance establishing said commission; and

WHEREAS, Section 601 of the City Charter entitled "Boards and Commissions," reserves to the City Council the authority to create boards and commissions by ordinance, and to prescribe their function, duties, powers, jurisdiction and the number of board and commission members, their terms, compensation and reimbursements for expenses, if any; now, therefore

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

SECTION 1. ESTABLISHMENT

Pursuant to Section 601 of the Charter of the City of Oakland, there is hereby created an Oakland Privacy Advisory Commission (hereinafter referred to as the "Privacy Commission" or "Commission").

SECTION 2. DUTIES AND FUNCTIONS

It shall be the duty and function of the Privacy Commission to:

a. Provide advice and technical assistance to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.

b. Conduct meetings and use other public forums to collect and receive public input on the above subject matter.

c. Draft for City Council consideration, model legislation relevant to the above subject matter, including a Surveillance Equipment Usage Ordinance.

d. Review and make recommendations to the City Council regarding any proposed changes to the operations of the Domain Awareness Center ("DAC") and/or proposed changes to the City's Policy for Privacy and Data Retention for the Domain Awareness Center ("DAC Policy") as specified in Resolution 85638 C.M.S.

e. Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.

f. Provide analyses to the City Council of pending federal, state and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.

g. The Privacy Commission shall make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate. An annual report will be presented in writing to the City Council. The Commission may submit recommendations to the City Council following submission to the City Administrator.

SECTION 3. MEMBERSHIP AND QUORUM

a. The Commission shall consist of nine (9) members, at least six (6) of whom are Oakland residents. Pursuant to Section 601 of the Charter, members of the Commission shall be appointed by the Mayor subject to confirmation by the affirmative vote of five members of the Council. Each Councilperson may recommend to the Mayor his/her own selection for Commission member.

b. Five (5) members shall constitute a quorum.

c. Each commission member shall serve as a volunteer without pay.

d. The members shall be appointed to overlapping terms of three (3) years beginning on March 15th of each year and ending on March 15th three years later, or until a successor is appointed and confirmed pursuant to Section 601 of the City Charter. An appointment to fill a vacancy shall be for the unexpired term only. To assure that terms overlap, appointments shall be as follows: three (3) initial members will serve a three-year initial term, three (3) initial members will serve a two-year initial term, and the other three (3) initial members will serve a one-year initial term.

e. In the event an appointment to fill a vacancy has not occurred by the expiration of a member's term, that member may remain in a holdover capacity for up to one year only following the expiration of his or her term or until a replacement is appointed, whichever is earlier.

f. No member of the Privacy Commission shall serve more than three (3) consecutive terms.

g. All members of the Privacy Commission shall be persons who have an interest in privacy rights as demonstrated by work experience, civic participation, and/or political advocacy. No member may be an elected official. Members of the Privacy Commission shall represent the following criteria, with no more than two (2) members representing any one criteria and at least one from each criteria to the extent possible:

1. an attorney, legal scholar, or activist with expertise in privacy, civil rights, or a representative of an organization with expertise in the same such as but not limited to the American Civil Liberties Union, the Electronic Frontier Foundation, and the National Lawyers Guild;

2. a past or present member of member of law enforcement who has worked with surveillance equipment and other technology that collects or stores citizen data;

3. an auditor or certified public accountant;

4. a hardware, software, or encryption security professional;

5. a member of an organization which focuses on government transparency and openness such as but not limited to the League of Women Voters or Open Oakland or an individual, such as a former government employee, with experience working on government transparency and openness.

h. No member may have a financial interest, employment, or policy-making position in any commercial or for profit facility, research center, or other organization that sells surveillance equipment or profits from decisions made by the Commission.

SECTION 4. VACANCY AND REMOVAL

a. A vacancy on the Privacy Commission will exist whenever a member dies, resigns, or is removed, or whenever an appointee fails to be confirmed by the Council within 60 days of appointment. Vacancies shall be filled for any unexpired term provided, however, that if the Mayor does not submit for confirmation a candidate to fill the vacancy within 90 days of the date the vacancy first occurred, the Council may fill the vacancy. If the Mayor does submit for confirmation a candidate to fill a vacancy within the 90-day time frame and the Council does not confirm the candidate, the 90-day period shall commence anew. For purposes of this Section, a seat filled by a holdover appointment will be considered vacant as of the expiration of the holdover's prior term of office.

b. Pursuant to Charter Section 601, a member may be removed for cause, after a hearing, by the affirmative vote of at least six (6) Council members.

SECTION 5. COMMISSION GOVERNANCE

a. OFFICERS AND ELECTIONS

At the first regular meeting, and subsequently at the first regular meeting of each year, members of the Privacy Commission shall elect a chairperson and a vice chairperson

b. MEETINGS AND VOTING

The Privacy Commission shall meet at an established regular interval, day of the week, time and location suitable for its purpose. Such meetings shall be designated regular meetings. Other meetings scheduled for a time or place other than the regular day, time and location shall be designated special meetings. Written notice of special meetings shall be provided to the Privacy Commission members and all meetings of the Commission shall comport with the Ralph M. Brown Act and the City's "Sunshine Ordinance" (Chapter 2.20 of the Oakland Municipal Code).

The Privacy Commission shall, in consultation with the City Administrator, establish bylaws, rules and procedures for the conduct of its business by a majority vote of the members present. Voting shall be required for the adoption of any motion or resolution.

Any action by the Commission shall be approved by a majority of members present provided a quorum exists.

c. STAFF

Staff assistance may be provided to the Privacy Commission as determined by the City Administrator pursuant to his or her authority under the Charter to administer all affairs of the City under his or her jurisdiction.

SECTION 6. SEVERABILITY

If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

SECTION 7. CODIFICATION

The City Clerk shall codify this ordinance upon approval of the code numbering as to form by the City Attorney.

SECTION 8. EFFECTIVE DATE

This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall be effective upon the seventh day after final adoption.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL-WASHINGTON, GALLO, GUILLEN, KALB, KAPLAN, REID AND PRESIDENT GIBSON MCELHANEY

NOES -

ABSENT -

ABSTENTION -

ATTEST: _____
LATONDA SIMMONS
City Clerk and Clerk of the Council
of the City of Oakland, California

Date of Attestation: _____

NOTICE AND DIGEST

AN ORDINANCE ESTABLISHING OAKLAND PRIVACY ADVISORY COMMISSION, PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, AND DEFINING THE DUTIES OF SAID COMMISSION

This Ordinance establishes the Oakland Privacy Advisory Commission in accordance with the requirements of Oakland City Charter section 601, which provides that the City Council shall create all advisory boards and commissions by Ordinance and that the Mayor shall appoint all board members subject to confirmation by the City Council.

This ordinance establishes the jurisdiction, duties, and powers of the Commission to provide advice and technical assistance on best practices to protect privacy concerns in the City's use of surveillance equipment and other technology that collects or stores citizen data. It further provides for the appointment, term, composition, membership qualifications, and the general rules and procedures for the Commission's meetings and deliberations.