CITY OF OAKLAND

AGENDA REPORT

TO: JOHN A. FLORES
INTERIM CITY ADMINISTRATOR

FROM: Joe DeVries

SUBJECT: DAC Privacy and Data Retention Policy

DATE: January 28, 2015

City Administrator Approval

Date 1/28/15

COUNCIL DISTRICT: City-Wide

RECOMMENDATION

Staff recommends that Council:

1. Accept this Report and adopt a Resolution: 1) affirming the right to privacy; 2) establishing the City of Oakland Domain Awareness Center (DAC) privacy and data retention policy which prescribes the rules for the use, accessing and sharing of DAC data; establishes oversight, auditing and reporting requirements; and imposes penalties for violations; and 3) authorizing the DAC to become operational

2. Consider additional policy recommendations which require future Council action from the DAC Ad Hoc Advisory Committee that will support the policy, assure ongoing compliance with the policy, establish penalties for violation of the policy, and potentially extend the components of the Policy to a broader range of City functions.

EXECUTIVE SUMMARY

The DAC Ad Hoc Advisory Committee developed this Privacy and Data Retention Policy, hereafter referred to as "the Policy" (Resolution, Attachment A) at Council's direction contained in Resolution No. 84869 C.M.S. which stated that "A data retention as well as a privacy policy shall be developed by the Council Approved Advisory Body prior to the activation of the Port-only Domain Awareness Center. The attached resolution affirms the City Council's direction and adopts the draft Policy as official City Policy.

Staff also requests that Council consider the accompanying recommendations for future council action from the Ad Hoc Advisory Committee, some of which are outside the authority of the

Staff also requests that Council consider the accompanying recommendations for future council action from the Ad Hoc Advisory Committee, some of which are outside the authority of the Advisory Committee but still relevant to the work of that body. These recommendations either support the Policy or further its purpose to encompass future City Technology:

1. Establish a Standing Privacy Policy Advisory Committee of the City to provide guidance to the City Council on potential changes to either the DAC or the DAC Privacy and Data Retention Policy.
2. Recommend to the City Administrator that a person is designated and shall serve as the Internal Privacy Officer within the DAC charged with ensuring the DAC Staff are abiding by the Policy, and that the City Auditor shall serve as the "Compliance Officer" who is responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer, and that the Public Ethics Commission shall serve as an Ombudsman/Advocate to receive complaints from whistleblowers or the general public and to make policy recommendations to the Advisory Committee and City Council.
3. Request the City Administrator or designee prepare an ordinance that makes violation of the Policy a misdemeanor punishable by fines and also enforceable by injured parties under a private right of action.
4. Determine that changes must be proposed by/to the Privacy Advisory Committee and ratified by the City Council and that Privacy policy must be reviewed at least every year by the committee.
5. Create a Permanent Standing Advisory Committee to examine the City as a whole and develop an overarching Privacy Policy that would reach beyond the limited scope of the DAC.
6. Modify the City's Whistleblower Ordinance to broaden protections and allow for more avenues to file a complaint when there is a DAC policy related potential violation.
7. Consider establishing a Citywide Surveillance Technology Ordinance to allow for informed public debate and decision making by the City Council regarding privacy and retention policies for all Surveillance Technologies in the future.

The attached Draft Policy is almost completely the product of the Ad Hoc Advisory Committee with the exception of three modifications that occurred after the last meeting of the committee. Those modifications are supported by the City Administrator and are as follows:

- On page one, a sentence that stated *"Therefore, the DAC and the entirety of this policy are exclusive to Port areas within Oakland"* was removed at the request of the Port because it was duplicative and because there was concern it would confuse the reader to assume the Policy covered internal Port operations which it does not.

  Also on page one, the last sentence of the Policy Purpose Section states, *"Notwithstanding any other language or statement contained herein, this Policy shall be limited to the actual activation of the joint City-Port DAC at the EOC located1605*

Martin Luther King Jr. Way, in Oakland, California by City staff whether acting solely or in conjunction with Port staff. Further this Policy does not prohibit the Port from monitoring Port properties by using security systems solely operated by the Port and outside of the City's control."

- This sentence was added to provide clarity for the reader that the DAC is located at the Emergency Operations Center (EOC) loeated at 1605 Martin Luther King Jr. Way, in Oakland, California and not at the Port of Oakland. This Policy does not apply to the Port's operation of its own security systems that the City has no control over and that are not housed at the EOC.
- The City Attorney has reviewed the language presented to the City extensively and, to add clarification, has reeommended that the following paragraph be added to the policy on page 2 as the last paragraph of the Policy Purpose Section: *Notwithstanding the provisions of this policy, the City the does not waive any right as provided by any relevant fedenal, state, or local law including but not limited to the California Public Records Act and the California Emergency Services Act. Further, the provisions of this policy do not relieve the City of any existing responsibilities, duties, or obligations as provided by any Memorandum of Understanding or Agreement for which the City is a party or any local, state, or federal law. Finally, nothing in this policy is intended to prohibit the DAC from being used as specified in Section VII.B or is intended to create a new privacy right for individuals beyond what is protected by the California and United States Constitutions.*

OUTCOME

Adoption of the Policy will satisfy the Council direction provided to staff on March 4, 2014 via City Council Resolution No. 84869 C.M.S. ensuring the development of a "Privacy and Data Retention Policy for the Domain Awareness Center (DAC)" before the DAC is made operational. This policy's purpose is to protect the Right to Privacy, civil liberties, and freedom of speech of the general public as well as erect safeguards around any data captured at the DAC when activated, and to protect against its improper use, distribution, and/or breach.

Adoption of **recommendations 1-4** from the Ad Hoc Advisory Committee above are directly related to portions of the Policy that cannot be enabled without further Council action including establishing enforceable consequences for violations of the Policy, establishing a reporting and auditing framework, and continuing ongoing citizen review.

Adoption of **recommendation 1**, which would require future Council action, would allow for the creation of a Standing Advisory Committee to oversee the work of the DAC specifically. Council would need to direct staff to prepare an Ordinance that delineates the membership and structure of the Committee per the City Charter, and the membership would not necessarily have the same members as the current Ad Hoc Committee.

Adoption of **recommendation 5** essentially expands the role of the Standing Committee (in recommendation 1) beyond the limited focus of the DAC to examine the City as a whole and provide recommendations to the City Council on a broader array of technology and develop an overarching Privacy Policy.

Adoption of **recommendation 6**, which would require future Council action, is to ensure greater opportunity to report abuses of the DAC Data or System; however, it is not required to make the Policy functional.

Adoption of **recommendation 7**, which would require future Council action, is seeking to make the decision making process regarding Surveillance Technology Citywide more public and thorough and expands the discussion outside the narrow scope of the DAC. It would serve as an opportunity to expand the principals of the attached Policy to a wider array of City functions and establish a more public process by which the decision to use new technology is reached.

BACKGROUND/LEGISLATIVE HISTORY

On March 4, 2014 the City Council adopted Resolution No. 84869 C.M.S. that stated, "A data retention as well as a privacy policy shall be developed by the Council Approved Advisory Body prior to the activation of the Port-only Domain Awareness Center. Members of the Advisory Body will be appointed by each member of the City Council."

Staff worked directly with the City Council Offices to identify individuals that had an interest in serving on the Ad Hoc Committee with a goal of appointing a balanced group that included people with expertise in areas such as privacy rights, civil liberties, technology, as well as individuals who represent Oakland's neighborhoods and business community.

The DAC Ad Hoc Privacy and Data Retention Advisory Committee conducted its inaugural meeting on May 1st, 2014. It began its work in an information-gathering stage requesting information from staff about: data security, information sharing agreements with outside agencies, situational capabilities and uses of the DAC in its currently proposed form, as well as further analysis of current data retention policies. While this information gathering occurred, the committee also defined a set of core principles that the policy needed to include.

In July, the Committee applied its core principals to the draft Privacy Policy Framework that staff had developed in the winter of 2013 and began redrafting the policy. The Committee ultimately met 18 times over six months to produce the final draft Policy **(Attachment A)** for Council consideration. The Committee also formulated the aforementioned 6 recommendations for the City Council to consider that will support the policy in varying ways, and one

recommendation to further the purpose of the Policy to a broader spectrum of future City Technology.

Prior Council action did not commit any operational funding to the DAC for any type of staffing plan. However, the Port of Oakland previously reeeived and acoepted Federal grant funds for the eventual staffing of the first two years of operation of the DAC as it was originally envisioned as a joint City-Port project. Port staff has since examined various staffing scenarios, including a no new City staff option. Based on scope changes to the DAC, including the direction of Council to implement a Port-only approach, and as a result of on-going discussions with the City, the Port Board of Commissioners directed staff to request that Port Security Grant Program (Round 13) funds be reprogrammed to support staffing of existing Port security systems on Port property.

Grant funds will be used to support and manage in-house capabilities at the Port of Oakland has an affirmative obligation under Federal law to continuously monitor its facilities and its approaches on land and water. The Port's Video Monitoring Systems Use Policy will govern use and access to the system.

The DAC Policy will remain intact. However, the DAC system will not be monitored in a continuously active state at the Emergency Operations Center (EOC) by either City or Port staff. Instead, the DAC Policy will only apply if and when the DAC System is activated at the City-owned facility located at Martin Luther King, Jr. Way for any of the many situations identified in Section VIII A of the Policy. Due to this change in anticipated operational use, minor editing changes to the language of the Policy are still required.

ANALYSIS

The creation of the DAC in Oakland, through grant funding from the Department of Homeland Security at a time when the Federal Government's efforts at gathering massive amounts of data about Americans was revealed by Edward Snowden, created a unique local flashpoint in 2013. This serendipitous moment has allowed for a debate to unfold about how Oakland will protect people's civil liberties and personal freedoms in an era of significant expansion of surveillance technology that is designed to more efficiently protect public safety.

The City Council's motion to restrict the scope of the DAC in March of 2014 and create an Ad Hoc Advisory Committee to develop a Privacy and Data Retention Policy has allowed that discussion to unfold in regard to a very practical application. The committee was given a narrow task of developing a policy for a specific technology but the committee members remained conscious throughout the process of the need to be able to apply this policy to a broader array of technologies both currently as well as into the future with technology that has yet to be developed.

Therefore, the committee produced a policy that proactively identifies how the technology can be used, how it can be modified, who has oversight over the process, and what course of action should be taken when the policy is violated.

The key points of the Policy include: 1) Data Sharing limitations with outside agencies, 2) Who has a Need and/or Right to the data, 3) Specifically what uses of the DAC are permissible, 4) What is considered "Protected Activity," 5) How oversight and reporting will occur, and 6) What penalties exists to deter people from violating the Policy. Although the Policy clearly delineates these functions, there is a need for the City Council to make certain determinations that were outside the jurisdiction of the Ad Hoc Committee for the Policy to be enabled. Also, the City Administrator, Public Ethics Commission, and City Auditor would have to make certain determinations for all provisions of the policy to become effective. These are listed below:

1. ***Establish a Standing Privacy Advisory Committee of the City for the DAC***

There are four distinct roles that the Ad Hoc Advisory Committee recommends the City fill to ensure a system of checks and balances exists for the DAC to avoid abuses of the system. The first of which is a Standing Privacy Policy Advisory Committee that would provide guidance to the City Council on potential changes to either the DAC or the DAC Privacy and Data Retention Policy. This committee would also make assessments of new technology that could impact the policy, review annual compliance reports, and provide a venue for public comment. This body's recommendations would be required before the City Council hears any potential changes to the DAC.

2. ***Identify the Internal Privacy Officer, Compliance Officer, and Ombudsman/Advocate***

The three remaining roles that the Ad Hoc Committee recommends the City identify are recommended as follows:

a. Internal Privacy Officer: the Committee strongly recommends to the City Administrator that they designate a person to serve as the Internal Privacy Officer within the DAC who is charged with ensuring the DAC Staff are abiding by the Policy on a day-to-day basis. They would be required to check the logs, file reports, and make immediate decisions that arise that do not allow time for a further review. Because the DAC is housed within the EOC, The EOC Manager would be the most likely candidate for this role.
b. Compliance Officer: The City Auditor or their designee should serve as the "Compliance Officer" who is responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer and should conduct random audits to ensure the DAC Staff is abiding by

the Policy. The committee recommends that the Auditor serve in this capacity as it is synonymous with the Auditor's role as defined in the City Charter.

c. Ombudsman/Advocate: the Committee recommends that the Public Ethics Commission should serve as an Ombudsman/Advocate. This is recommended to ensure there is an entity outside the City's normal chain-of-command that is both available to receive complaints from whistleblowers or the general public and also to make policy recommendations to the Advisory Committee and City Council. Although this role is not as well fitted as the role the committee identified for the Auditor, it does fit as an outside body that has a degree of authority outside the typical Political or Administrative City functions.

3. Request the City Administrator or designee prepare an ordinance that makes violation of the Policy a misdemeanor punishable by fines as well as a private right of action by the injured party

The Committee wrote penalties directly into the Policy to ensure DAC staff would understand the severity of their actions if they were to misuse the data or technology. The Policy currently states that violations are considered a misdemeanor punishable by up to one year in jail or a fine of up to $1000. This language is compatible with the City Charter requirement that misdemeanor fines are capped at $1000. In order for this provision to be enforceable, an Ordinance would need to be adopted by the City Council stating so.

The Committee also wanted to acknowledge that when someone's personally identifiable information is misused it is an injury that could ultimately prove very costly therefore; the Committee is recommending that these violations cause the violator to be subject to a Private Right of Action.

Both of these portions of the Policy would require a meet and confer with the City's labor organizations and this process would need to conclude before the full City Council can adopt the Policy.

4. Changes to the Policy

Changes must be proposed by staff first to the Privacy Advisory Committee and subsequently ratified by the City Council or the proposed changes should originate *from* the Privacy Advisory Committee and subsequently ratified by the City Council. No changes should be made without this public review process. The Privacy Policy must be reviewed at least every year by the committee.

5. Create a Permanent Standing Advisory Committee

The Committee believes the City should establish a Standing Advisory Committee to examine the City as a whole and develop an overarching Privacy Policy that would reach beyond the limited scope of the DAC. This could be the same body as the committee recommended in section 1 but with a much broader purpose. This could also be the entity that develops a Citywide Surveillance Technology Ordinance as recommended below in #8. This body should be sufficiently prepared to consider new technology and compliance with state and federal laws in the ever changing world of data collection and management.

6. Modification of the City's Whistleblower Ordinance

The Committee recommends certain modifications to the City's current Whistleblower Ordinance (No. 12890 C.M.S.) that would require future Council action and are as follows:

Amend: 2.38.020 "Whistleblower" defined to include any *person* instead of any *officer or employee* reeognizing that retaliation against a contractor or volunteer within the City's organization could stifle whistleblowing:

The current definition:

> "Whistleblower" is defined as an officer or employee who reports or otherwise brings to the attention of the City Auditor any information which, if true, would constitute one of the following: a work-related violation by a City officer or employee of any law or regulation; fraud, waste or mismanagement of City assets or resources; gross abuse of authority; a specific and substantial danger to public health or safety due to an act or omission of a City official or employee; or use of a City office, position or resources for personal gain.

The recommended change to the definition:

> "Whistleblower" is defined as *any person* who reports or otherwise brings to the attention of the City Auditor *or Public Ethics Commission* any information which, if true, would constitute one of the following: a work-related violation by a City officer or employee of any law or regulation; fraud, waste or mismanagement of City assets or resources; gross abuse of authority; a specific and substantial danger to public health or safety due to an act or omission of a City official or employee; or use of a City office, position or resources for personal gain.

The Committee also recommends the following addition to this section:

Any Whistleblower complaint arising from an act governed by the Domain Awareness Center ("DAC") Privacy and Data Retention Policy may be made to the City Auditor, the Public Ethics Commission, the DAC Privacy Policy Advisory Committee, the DAC Standing Advisory Committee, the DAC Compliance Officer, or the DAC Ombudsman/Advocate.

All other Whistleblower complaints shall be made to the City Auditor.

Any Whistleblower complaint made pursuant to this chapter shall be immediately investigated by the City Auditor or Public Ethics Commission.

This addition would allow for more "doors" through which to file a complaint and draws more eyes to a problem, especially if an employee or other person was uncomfortable coming forward to any particular entity listed.

Amend: 2.38.030 Whistleblower identity

Current Language:

To the extent permitted by law, the identity of anyone reporting information to the City Auditor about an improper government action shall be treated as confidential unless the employee waives his or her confidentiality in writing.

Proposed Language:

To the extent permitted by law, the identity of the *whistleblower* shall be treated as confidential unless the employee waives his or her confidentiality in writing.

This change would simply cleans up the old confidentiality section to be more general to ensure that anyone's identify will be protected regardless of what they are reporting and who they are reporting it to.

The Committee recommends this new section: 2.38.120 Training

All managers, supervisors, and department heads shall undergo periodic training about whistleblower protections, retaliation, and appropriate methods to address employee concerns.

The Committee feels that there needs to be a training of managers and supervisors within the City to ensure they are familiar and compliant with the law.

7. Citywide Surveillance Technology Ordinance

The Committee determined that the City of Oakland currently lacks a process that fully informs the public and enables the Council to make an informed decision about the proposal, acquisition, and use of surveillance technologies by City entities. The Committee recommends that the City Council adopt an ordinance that applies to all City entities and provides for at least the following:

Informed public debate and decisions by the City Council about Surveillance Technology Proposals: Public notice, distribution of information about the proposal, and public debate *prior to* seeking funding or otherwise moving forward with surveillance technology proposals could prove critical to avoiding costly and divisive debates in the future in which the interests of public safety and protection of grant funding is pitted against the interests of full disclosure and civil liberties.

The City Council could facilitate this informed public debate, expressly consider costs (both fiscal and to civil liberties), and determine that surveillance technology is appropriate or not before moving forward with any proposal.

Privacy and Retention Policies for All Surveillance Technologies: Legally enforceable Privacy and Retention Policies with robust civil liberties, civil rights, and oversight safeguards similar to the DAC Policy could be considered and approved by the City Council for each surveillance technology before use.

Ongoing Oversight & Accountability of Its Use: Proper oversight of surveillance technology use and accountability through annual auditing and public reporting and oversight, by the public and the City Council could be required as it is in the DAC Policy.

If the Council does create a Standing Advisory Committee, the Committee's charge could be to begin the process of developing such an ordinance as the first component of its work. This idea is gaining traction throughout the Bay Area and California as more and more cities are wrestling with the increased use of new technologies by law enforcement agencies taking place in a new arena of public policy.

Policymaking bodies have faced challenges keeping up with technological advances that are often funded by federal grant dollars. Local governing bodies, in competing for and accepting grant funding for such technologies, sometimes inadvertently fail to thoroughly and publicly vet the impacts of purchasing and using such technology. A Citywide Surveillance Ordinance could remedy this gap and provide the public with a greater sense of security that their privacy interests are being protected by the City. Throughout the process of developing the DAC Privacy and Data Retention Policy, the Committee Members maintained an understanding that their work could be applied to the City as a whole and the vote to make this recommendation passed unanimously.

PUBLIC OUTREACH/INTEREST

The Ad Hoc Committee was created by Council action due to widespread interest in this issue and an overwhelming outpouring of public speakers when the Council was considering accepting Federal grant funds to finance the construction of the DAC. All meetings of the Committee about the Policy were properly noticed with the City Clerk. Staff also created an email distribution list so that any interested party received all of the agenda materials at the same time as the committee members.

COORDINATION

The City Administrator provided direct staff support to the committee and the following departments also regularly participated and assisted in the preparation for the Advisory Committee Meetings and the Policy those meetings ultimately produced: the Department of Information Technology, City Clerk, City Attorney, Police Department, Fire Department, and the Office of Emergency Services. The City Attorney's Office, the Port of Oakland and Budget Office were consulted in the preparation of the DAC Policy and this report.

COST SUMMARY/IMPLICATIONS

This report has no direct fiscal impact. However, the adoption of some of the recommendations could have a fiscal impact in that they would require staff support on an ongoing basis.

SUSTAINABLE OPPORTUNITIES

Economic: No economic opportunities are identified in this report.

Environmental: No environmental opportunities are identified in this report.

Social Equity: The development and adoption of a privacy policy provides residents with an indication that the City is responding appropriately to concerns about the Domain Awareness Center's impact on residents' civil liberties and is establishing safeguards to prevent potential abuse of the technology or the data collected by the DAC.

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

Attachments:
A- Final Draft Privacy and Data Retention Policy for the DAC.
B- Resolution establishing the Domain Awareness Center Privacy and Data Retention Policy

Item: _____
Public Safety Committee
February 10, 2015

Approved as to Form and Legality

City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO. _____ C.M.S.

Introduced by Councilmember _____

RESOLUTION: 1) AFFIRMING THE RIGHT TO PRIVACY; 2) ESTABLISHING THE CITY OF OAKLAND DOMAIN AWARENESS CENTER (DAC) PRIVACY AND DATA RETENTION POLICY WHICH PRESCRIBES THE RULES FOR THE USE, ACCESSING AND SHARING OF DAC DATA; ESTABLISHES OVERSIGHT, AUDITING AND REPORTING REQUIREMENTS; AND IMPOSES PENALTIES FOR VIOLATIONS; AND 3) AUTHORIZING THE DAC TO BECOME OPERATIONAL

WHEREAS, on March 4, 2014, the City Council passed Resolution No. 84869 C.M.S., which restricted the use and application of Oakland's Domain Awareness Center (DAC) to the monitoring of Port of Oakland property and surrounding areas; required the development of a Privacy and Data Retention Policy before the DAC Phase II could be made operational; and the Council also approved an Ad Hoc Community Advisory Committee made up of City Council appointees, charged with the development of this Policy; and

WHEREAS, the Ad Hoc Advisory Committee held several meetings in which representatives of various City departments participated, the Advisory Committee has finalized their proposed Privacy and Data Retention Policy through an open and accessible public process, which Policy is attached to this Resolution; and

WHEREAS, the purpose of this Policy is to ensure that individuals' rights to privacy, civil liberties, and freedom of speech are protected by establishing rules for the collection, use, retention, and sharing of DAC data; by erecting safeguards against the improper use, distribution, and/or breach of DAC data and systems; and by requiring appropriate levels of oversight, reporting and transparency; and

WHEREAS, upon Council's adoption of a DAC Privacy and Data Retention Policy and the completion of the DAC Phase II process, the DAC will be brought into operation enabling the City to access situational awareness information so that the City is better equipped to make timely and critical decisions on the best ways to prevent, prepare for, respond to, and recover from emergencies and potentially catastrophic events; and

WHEREAS, this Policy applies 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 within their jurisdiction and control; now therefore be it

RESOLVED: That the City of Oakland affirms an individual's right to privacy as recognized in the California and United States Constitutions; and be it

FURTHER RESOLVED: That the City Council hereby adopts the proposed DAC Privacy and Data Retention Policy recommended by the Ad Hoc Community Advisory Committee, which is attached, as the City of Oakland's official DAC policy; and be it

FURTHER RESOLVED: That this Policy shall be implemented as prescribed and the City Administrator shall adopt rules and regulations and take any other action necessary to implement and administer this Policy.

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

[PROPOSED] CITY OF OAKLAND DOMAIN AWARENESS CENTER (DAC) PRIVACY AND DATA RETENTION POLICY

I. BACKGROUND AND OVERVIEW

Port Domain Awareness Center (interchangeably referred to in this document as 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 information 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, 2009.

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.

"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 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.

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.

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.

II. MISSION OF THE DOMAIN AWARENESS CENTER

The mission of the DAC is to provide situational awareness information so that the City is better equipped to make timely and critical decisions on the best ways to prevent, prepare for, respond to, and recover from emergencies and potentially catastrophic events.

III. POLICY PURPOSE

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 protects all people's privacy and civil liberties.

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 decision free from any force that has violated our secrecy or anonymity.

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.

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.

IV. UPDATES TO THE POLICY AND TO DAC

A. City Council shall establish a permanent Privacy Policy Advisory Committee for the DAC. 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.

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 less 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 City Council, through passed resolution 84869 on March 4th, 2014, which provides in relevant part the following limitations on the Domain Awareness Center:

That the Domain Awareness center will be implemented in a port-only approach and shall hereafter be referred to as the "Port Domain Awareness Center (DAC); and . . .

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, and . . .

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, and . . .

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 . . .

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

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, and . . .

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 . . .

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 . . .

V. DEFINITIONS

As used in this Policy, the following terms are defined below:

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

"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 video management systems that allows DAC Staff to quickly mark and annotate a moment for later review; the time stamped record is the bookmark.

"Compliance Officer" means the City Auditor or their designee who is responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer and conducts random audits to ensure the DAC Staff is abiding by this Policy.

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

"DAC Operations Group" means the various personnel who support and maintain the DAC IT systems.

"DAC Staff" means the City of Oakland employees who will be responsible for monitoring the equipment within the DAC on a day-to-day basis, 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 or framework: Port Security Cameras (Phase 1), Port Intrusion Detection System (IDS) (Phase 1), Port 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), NOAA Weather Alerts (Phase 2), 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 or framework.

"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."

"Internal Privacy Officer" means the person who oversees the day-to-day operations of the DAC and who is charged with ensuring the DAC Staff are abiding by this Policy on a day-to-day basis. They check the logs, file reports, and make immediate decisions that arise that do not allow time for a further review.

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

"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, or 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 requires 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 Record Keeping and Auditing requirements under Section IX.

"Personally Identifiable Information" (called 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, 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 not 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.

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.

VI. ACCESS TO THE DAC SYSTEM / EQUIPMENT

Day to Day Operations

The DAC computer and network equipment is maintained by the City's DAC Operations Group.

Only DAC Staff will be used to monitor DAC Data. All employees who are assigned to monitor the DAC Data will be required to undergo security background checks at the local level as well as security clearances at state and/or federal levels and will be required to sign binding Non-Disclosure Agreements to ensure data and information security.

Training

Training by the Internal 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.

Critical incidents/emergencies/EOC activations

During an Allowable Use as enumerated in Section VIII.A. with EOC activation, notwithstanding the requirements in Section VII, City of Oakland Agency Directors and/or their designees in the Emergency Operations Center (EOC) and outside governmental agencies and non-governmental agencies' staff assisting with the Allowable Use (such as the Red Cross) that would report to EOC may have limited access to the live data produced by the DAC System only on a Need To Know basis and if there was a direct correlation between the Allowable Use and DAC operations.

Support and Repairs

ITD staff and vendors that installed the systems as well as other maintenance providers will have access to the system components but will be prohibited from access to DAC data. Various manufacturers and vendors are hired to provide additional support services. Any system and network level access by these vendors require both a background check and ITD employee presence. 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.

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.

VII. 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 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 unless the City is required by law to provide such information directly to the requestor. 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 in Section VIII.

VIII. ALLOWABLE USE

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
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 also 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 Internal Privacy Officer no later than 8 hours after activation of the DAC System.

IX. AUDITS AND REPORTING METRICS

Because surveillance technology invites abuse by persons with access to its tools and data, the DAC shall be periodically audited for compliance with this Policy.

Internal Recordkeeping, Auditing, and Internal Privacy Officer

It is recommended that a City official or designee serve as an Internal Privacy Officer. Such an official shall oversee the day-to-day operations of the DAC and will be charged with ensuring the DAC staff is abiding by this policy on a day-to-day basis. Further, such official shall check the logs, file reports, and make immediate decisions that arise that do not allow time for a further review and shall be responsible for preparing the Internal Recordkeeping and Audits and ensuring DAC Staff compliance with this Policy.

The results of Internal Auditing shall be provided to the Compliance Officer, City Administrator, the City Council, and be made publicly available to the extent the release of such information is not prohibited by law.

DAC Staff shall keep the enumerated records in this section for a period of 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 the following:

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).

External Audits/Public Safety Effectiveness

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:

1. **Purpose Specification**: General statistical breakdown of how the DAC System was used including:
    a. Listing and number of incident records by incident category
    b. Average time to close an incident record
    c. Number of incidents actionable by DAC Staff vs. number of incidents non-actionable and/or false alarms.
2. **Public Safety Effectiveness:** Summary and general information and evaluations about whether the DAC has accomplished its stated purpose, including:
    a. Crime statistics for geographic areas where the DAC was used;
    b. The number of times the DAC was used to bookmark or retain data for potential criminal investigations;
    c. The number of times DAC Data was shared for potential criminal investigations;
    d. Lives saved;
    e. Persons assisted;
    f. Property saved or preserved;
    g. Wildlife/Natural Habitat saved or assisted.
3. **Data Sharing:** How many times DAC Data was shared with non-City entities and:
    a. The type of data disclosed;
    b. Justification for disclosure (e.g., warrant, memoranda of understanding, etc.)
    c. The recipient of the data;
    d. Date and time of disclosure; and
    e. Obligations imposed on the recipient of shared information.
4. **Data Minimization:** Describe whether and how the DAC System was used in a manner not allowed under Section VIII A of this Policy. Describe whether and how the DAC Data was accessed in violation of this Policy and what were the consequences of such misuse?
5. **Protected Activity Exception:** The number of times DAC Staff certified use of the Protected Activity Exception as provided in Section VIII B, and copies of each written certification.
6. **Dispute Resolution:** A summary and description of the number and nature of complaints filed by citizens or whistleblowers and the resolution of each.
7. **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 including whether the City approved or rejected the proposal and/or required changes to this Policy before approval.
8. **Data Retention:** Describe whether data was retained in violation of this Policy.
9. **System Access Rights Audit**: Verification that individual user assigned access rights match access rights policy for user's designated staff role.
10. **Public Access:** Statistics and information about public records requests received, including response rates.
11. **Cost:** Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs.

Independent Audits

The City Council shall provide for annual independent third party audits of DAC performance and security. The auditor shall have full access to Internal Recordkeeping, the DAC System, and

the DAC Data. The results of the independent audit shall be made publicly available online to the extent the release of such information is not prohibited by law.

Annual Report

The Compliance Officer shall prepare and present an Annual Report that summarizes and includes the results of **Internal Recordkeeping and Auditing, External Audits, and Independent Audits** to the extent the release of such information is not prohibited by law, and present it to the City Council at a public meeting in January of each year, or at the next closest regularly scheduled council meeting. The City Council should use the Report and the information it's based on to publically reassess whether the DAC benefits outweigh the fiscal and civil liberties costs.

X. RECORDS MANAGEMENT

The DAC 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.

DAC Staff must follow all relevant and applicable policies, procedures, regulations and laws.

XI. REDRESS AND PUBLIC INFORMATION REQUESTS

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.

XII. SANCTIONS AND ENFORCEMENT REMEDIES

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.

Further, contingent on the City Council passing legislation providing for a criminal penalty and/or private right of action as a consequence of a violation of this policy, the following provisions may apply. These provisions are noted by asterisks to indicate that they require further Council action to take effect

Criminal Penalty*

Any Person found guilty of knowingly or willfully violating any section or provision of this Policy shall be guilty of a misdemeanor and punishable upon conviction by a fine of not more than $1,000 or by imprisonment not to exceed six months, or both fine and imprisonment. This Policy defines any violation of this Policy as an injury to any person affected by such violation.

Private Right of Action*

There is a strong, definitive relationship between PII and the individual in that PII belongs to the individual (is considered their property) and is his/hers to disclose or to keep private to himself.

Any Person who knowingly or willfully violates any section or provision of this Policy, including without limitation the dissemination of PII, shall be subject to a private right of action for damages or equitable relief, to be brought by any other person claiming that a violation has injured his or her business, person, or reputation including mental pain and suffering they have endured. A person so injured shall be entitled to actual and punitive damages, a reasonable attorney's fee and other costs of litigation, in addition to any other relief allowed under California law. This Policy defines any violation of this Policy as an injury to any person affected by such violation.

XIII. SEVERABILITY.

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.