CITY OF OAKLAND

AGENDA REPORT

TO: JOHN A. FLORES
INTERIM CITY ADMINISTRATOR

FROM: Joe DeVries

SUBJECT: Supplemental Report on the DAC Privacy and Data Retention Policy

DATE: April 30, 2015

City Administrator Approval

Date 4/30/15

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 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.

REASON FOR SUPPLEMENTAL REPORT

On February 10, 2015 the Public Safety Committee asked staff to post the draft DAC Privacy and Data Retention Policy (the "Policy") and additional recommendations online to allow 30 days for public comment and publicize the comment period on the City's webpage. The Committee also asked staff to bring this item back to the Committee for further review on April 14, 2015. Last, the Committee requested staff to provide a written analysis of the implementation of the additional seven (7) recommendations made by the DAC Ad Hoc Advisory Committee (Advisory Committee).

Item: _____
Public Safety Committee
May 12, 2015

In response to the Council direction, staff posted the draft Policy and the additional recommendations on the city's website and received 55 public comments ***(Attachment A).*** Many commenters expressed strong support for the Policy and the additional recommendations. Specifically, there was almost unanimous support for the creation of a Permanent Standing Privacy Committee and the development of a Surveillance Technology Ordinance.

The Advisory Committee reconvened five (5) more times since the February 10th Public Safety Committee and invited input from the City Auditor, the Executive Director of the Public Ethics Commission (PEC), the Director of Employee Relations, and continued input from the Police, Information Technology, and Fire Departments. Staff worked internally to address concerns raised during the process, and staff further analyzed the Additional Recommendations brought forward by the Advisory Committee. This analysis is provided below:

Advisory Committee Recommendation 1:

Establish a Standing City Privacy Policy Advisory Committee to provide guidance to the City Council on potential changes to either the DAC or the DAC Privacy and Data Retention Policy.

Staff Analysis:

The current work of the DAC Ad Hoc Advisory Committee was limited in scope as was the DAC itself at the March 4, 2014 City Council Meeting. The DAC in its current operational form will not likely be activated very often and when it does, the allowable uses are very specific. Still, the importance of an oversight body to monitor and make recommendations about the DAC has value in that it can establish and maintain the public's trust that the City is committed to protecting civil liberties.

Staff Recommendation:

The creation of a Standing Committee for this limited role would be an inefficient use of City resources. Instead, staff recommends combining the oversight discussed in this recommendation with recommendation #5 below (creation of a Citywide Permanent Standing Advisory Committee).

Advisory Committee Recommendation 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.

Staff Analysis:

In further analysis of this recommendation, the DAC Advisory Committee met with the City Auditor on two separate occasions and made modifications to the current draft Policy based on the Auditor's input. These changes are most relevant in Section IX and can be seen in a redlined format ***(Attachment B).*** The effect of these changes is an amended recommendation by the Advisory Committee to modify the Policy in the following ways:

a. Instead of recommending an Internal Privacy Officer who oversees DAC day-to-day operations, the Committee is recommending a Chief Privacy Officer (CPO) who is a senior level administrator within the City of Oakland and is responsible for managing the risks and business impacts of privacy laws and policies for the City as a whole. The Committee envisions these responsibilities would be assigned to an existing staff person; however, such an assignment would decrease staff capacity for other items.

b. Instead of recommending that the City Auditor serve as the Compliance Officer, the role of Compliance Officer is designated to the internal staff member who oversees the DAC day-to-day operations. This is the role originally designated as the Internal Privacy Officer. The City Auditor, in this scenario, retains their authority to conduct perform audits as they see fit based on the data provided to them by the Compliance Officer without taking on a new duty that may be outside their charter-defined function.

The Executive Director of the Public Ethics Commission (PEC) spoke before the Advisory Committee. The Chair of the Advisory Committee and City Administrator's Staff also presented the draft Policy to the PEC, listening to their concerns about the proposed increased duties for the PEC. As referenced in the attached letter from the PEC ***(Attachment C)*** the PEC is concerned about taking on a new potentially time-consuming role that would require subject matter expertise that the PEC may not have. This is especially true at this time because the PEC is expanding its role with the recent passage of Measure CC last fall.

Staff Recommendation:

The changes to both the Policy and the Additional Recommendation regarding the designation of a Privacy Officer and Compliance Officer were made by the Advisory Committee in close collaboration with the City Auditor and therefore the City Administrator recommends these changes. Further analysis of the potential fiscal impact of designating a Privacy Officer needs to be considered if this person's duties would also

include serving as staff to a Standing Advisory Committee (Additional Recommendation #5).

Also, based on the input from the PEC, the City Administrator's recommendation is to currently not ask that the PEC serve in this additional capacity but to leave the option open for possible future PEC involvement in issues related to Privacy.

Advisory Committee Recommendation 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.

Staff Analysis:

There are several concerns regarding this recommendation for the City's Employee Relations (ER) Department. The ER Director met with the Advisory Committee in an effort to address these concerns. She stated that the recommendation for a specific City policy to explicitly create criminal and civil penalties for violations is extremely unusual. There are Just Cause standards that need to be reviewed on a case-by-case basis for any situation where a City considers disciplining or terminating an employee and in California employees have a property right to their job and are entitled to due process. Additionally, regardless of what is written in the Policy, all public employees can be terminated for cause *and can also be held criminally and civilly liable for their actions depending on the offense.*
Additionally, there is a clear obstacle to the adoption of the draft Policy in regard to the Meet and Confer requirements the City is bound to by its Memoranda of Understanding with its several unions. Before the City could add a new disciplinary requirement for its employees, all of the affected unions would have to agree to it and if any of them did not, the provision would be decided by an arbitrator if the City and the Union reached impasse. The ER Director believes the likelihood of the City prevailing in such arbitration is very low.

Staff Analysis:

The Advisory Committee did not modify the proposed draft Policy, but in light of the aforementioned obstacles and because current rules governing the workplace provide ample penalties for employees who violate City policy, the City Administrator is recommending that this provision not be adopted.* As a compromise, the City Administrator would recommend retaining the first paragraph of Section XII that mentions the fact that violations of City Policy can result in several levels of discipline (including criminal penalties) but remove the remaining four paragraphs that provide an explicit criminal penalty and private right of action associated with this specific policy.

**This compromise recommendation would require staff to modify Section XII (Sanctions and Enforcement Remedies) before final City Council adoption of the Policy.*

Advisory Committee Recommendation 4:

Determine that changes to the Policy 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.

Staff Analysis and Recommendation:

Staff supports adopting this recommendation to ensure a thorough and informed discussion about any changes to the DAC or the Policy governing its use. Due to its originally designed capabilities, the DAC could receive a much larger amount of data from the entire City and there were discussions of connecting it to many data sources prior to the March 4, 2014 City Council action. Due to the controversy surrounding the DAC and the lack of a Privacy Policy, this conversation was met with fierce opposition from the community and the current public comments on the Privacy Policy still allude to that opposition. However, there will continue to be other functions that could enhance public safety by adding them to the DAC that are not in the current Policy. For example, if a large building was on fire and the building plans were readily accessible to the DAC staff, they could identify where the gas main is located and help firefighters navigate safely. Because new functions could be identified at any time and the world of technology is ever changing, establishing a process now that requires public discourse into the future is recommended.

Advisory Committee Recommendation 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.

Staff Analysis and Recommendation:

Staff supports this recommendation for a number of reasons including those stated above under recommendation #1 regarding a standing committee for the DAC. The City will continue to seek and accept grant funding from the federal and state government to enhance its public safety capabilities. New technology is introduced into the marketplace every year that changes the conversation about how society is monitored. By establishing a Citywide Standing Privacy Committee the City will create a public space and process where this conversation can take place. The City can work in partnership with affected operational staff, privacy experts, and advocates to develop a mutually agreeable process to acquire new technology. The recent debate at the City Council about accepting grant

funds for the purchase of a Forward Looking Infrared Camera (FLIR) is a good example of how a standing committee could help the City move forward in a consistent, clearly defined, and transparent manner in the future.

Similar to establishing any permanent standing committee, staff would need to return to Council with an Ordinance delineating the Committee's size, scope, and composition. Staff anticipates that the Commission will require about 10-15 staff hours per month to support monthly meetings of the Committee. 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 Committee members, and developing reports and recommendations to the City Council.

This time would likely be absorbed by exiting staff although it would decrease staff capacity for other items. Depending on the extent of work created for a Privacy Officer (Advisory Committee Additional Recommendation #2), and if that same staff person served as the staff to this Standing Committee, this could have a fiscal impact. The fiscal impact could be a need for more staff to handle this role or other duties in need of reassignment due to increased focus on the privacy role. The City Administrator recommends closely tracking staff time dedicated to these functions and reassessing any increased fiscal impact after 6 months.

Advisory Committee Recommendation 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.

Staff Analysis and Recommendation:

The City's current Whistleblower Ordinance was written to be in line with State law regarding a reporting structure and the definition of who can be protected under such laws. The proposed changes from the Advisory Committee are attempting to do three different things:

a. The Advisory Committee proposes that the Council enact whistleblower type protections for persons who file complaints regarding non-compliance with the policy who are not City of Oakland employees who are covered under existing whistleblower laws. This would allow for volunteers, contractors or other non-city employees to be protected as Whistleblowers. This expands the definition of a Whistleblower beyond state law and at this time the City Administrator has requested the City Auditor evaluate this proposal and City Attorney determine whether it conflicts with state law on whistleblower protection for employees. At this time, the

Administration recommends waiting until that further analysis can be completed to ensure the City is not in conflict with State Law.

b. Allow for complaints to be received by the PEC, the DAC (or other) Privacy Advisory Committee, or the City Auditor. Based on the concerns identified by the PEC about modifying their role and the City's recommendation that a Standing Committee be more broadly defined (and not specific to the DAC) the Administration does not support this recommendation currently. Instead, the sole recipient of Whistleblower complaints should remain the City Auditor. This will maintain a consistent point of entry for complainants and does not preclude a Standing Committee, the PEC, or any other person from referring Whistleblowers to the City Auditor's Office when appropriate.
c. Require all managers, supervisors, and department heads to undergo periodic training about whistleblower protections, retaliation, and appropriate methods to address employee concerns. The administration supports this concept and employee protections such as the Whistleblower Ordinance are currently included in a new training series being developed by the Department of Human Resource Management.

Advisory Committee Recommendation 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.

Staff Analysis and Recommendation:

Staff recommends that the development of such an ordinance be the primary body of work for a Permanent Standing Privacy Committee once that Committee has been established and has had a reasonable period to establish itself and monitor adherence to the DAC Privacy Policy. This Committee will initially take some time to create procedures and a regular meeting schedule and it will be responsible for assessing the use of the DAC. It should have the medium-range goal of creating a framework for a Citywide Surveillance Technology Ordinance which could take several months. Developing such an ordinance will require input from the same departments that have been collaborating with the current Advisory Committee but would be much broader in its scope. The net effect would be to recommend an ordinance for adoption by the City Council that would establish a consistent public process by which the City evaluates various technologies *before* acquiring or using them.

Additional Modifications to the Draft Policy since the February 10 PSC Meeting

During the February 10th Public Safety Committee meeting, Council Member Brooks inquired as to whether City Council Members were permitted in the Emergency Operations Center during critical incidents in which the DAC is activated based on the current draft Policy. The Advisory

Committee discussed this question and decided to add additional language to the Policy that expressly allows for Council Members, the Mayor, and/or their designees to be present during such activations. However, the Committee included a recommendation to exclude the City Attorney from having access to the DAC data during a DAC activation at the EOC.

Staff Analysis

This proposal would not work with the City's Public Safety protocols for EOC activations. City Attorney staff--like other city departments – are required to respond to EOC activations and emergency response situations under the California Emergency Act, Gov. Code § 8550 et seq., and as provided by the City's Standardized Emergency Management System ("SEMS") regulations. During EOC activations Public Safety officials want and request that City Attorney staff report to the EOC to provide legal consultation in the context of a wide range of rapidly evolving scenarios. City Attorney input helps the City carry out its EOC operations in an expeditious and legal manner. Denying the City Attorney staff access to DAC data would hinder their ability to render legal advice to City staff on matters of DAC policy compliance and related legal issues. Moreover, the Oakland City Charter is Oakland's constitution and Section 401(6) of the Charter designates the City Attorney as the legal advisor to the Mayor, City Council, and each and every department of the City. The City Attorney advises all officers, boards, commissions, and other agencies of the City on legal matters. Accordingly, the City Attorney cannot be denied access to DAC data or any other information that is relevant or necessary to the provision of legal services.

Staff Recommendation

Staff recommends adding the words "City Attorney" to section VII to the draft policy before final adoption by the City Council.

ITD Staff worked closely with the committee to make other modifications to the current draft Policy to provide more clarity regarding the definition of a Bookmark, the access vendors would have to the system and its components, and other minor revisions. The current draft ***(Attachment D)*** contains all of the above mentioned changes.

Additional Concerns

The Police Department has expressed two unresolved primary concerns with the current Policy that will need continued monitoring:

The first concern expressed by the Police Department is the desire to potentially need to monitor a protest (Protected Activity) when it occurs at the Port. Although the Advisory Committee wrote an exception clause that allows monitoring of Protected Activity when there is a reasonable suspicion of criminal wrongdoing, the Police Department would like to be able to monitor such activity even when there is no reasonable suspicion. They have indicated that protests often lead to criminal activity that the department would not have had a reasonable suspicion that such activity would occur.

The second concern is the desire to have a more expansive list of Allowable Uses for the DAC. The Advisory Committee spent considerable time discussing the various Allowable Uses with Police, Fire, and Port staff, and created a list that includes Allowable Uses such as "Major Emergency." The Advisory Committee believes definitions such as this one offer Emergency Personnel broad latitude to use the DAC when needed, even in situations that were not contemplated during the deliberative process of developing the Policy.

Staff Recommendation:

The City Administrator recommends these concerns be tracked carefully to see what criminal activity occurs that could have been monitored by the DAC if the Policy were less restrictive and assess all of the protests at the Port that lead to criminal activity in the first year of operation. Ongoing and annual discussion of these types of incidents with the Standing Committee could result in proposed changes to the Policy as delineated in the Advisory Committee's Additional Recommendation #4.

It will take time for staff to return to Council with an ordinance creating a Standing Privacy Committee. The appointment of its members and regular scheduling of its meetings will also provide ample time for new data to be gathered about the impact of the Policy on DAC Operations. Furthermore, the development of a Surveillance Technology Ordinance will also be a deliberative process which will allow for even more information to be gathered about how the City should address its need to balance Public Safety and Security with Personal Liberties, neither of which need be mutually exclusive.

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

Attachment A: Public Comments on the Policy
Attachment B: Redlined Version of the Policy
Attachment C: Letter from the PEC
Attachment D: Final Draft of the Policy

Item: _____
Public Safety Committee
May 12, 2015

The DAC Policy and recommendations were presented at the February 10th Public Safety Committee Meeting and were posted to the City's website for public comment soon thereafter. The comments below represent all public comments received from March 2, 2015 and April 21, 2015.

I am an Oakland resident and encourage great caution in adopting any new surveillance technologies. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used.
I want to have a voice in the debate about surveillance and privacy in Oakland. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used.
I want to have a voice in the debate about surveillance and privacy in Oakland. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used.
I want to have a voice in the debate about surveillance and privacy in Oakland. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used. Thank you!
We are heading towards a "soft police state", we will be completely monitored thru electronic surveillance(bank accounts, emails, gps, cell phones, money, and license plates. At work we are monitored....is there anyway to preserve freedom and still live in the USA? Persevere to maintain freedom please. Barbara Smoak RN
I am an Oakland resident. Now is the time to put policies in place that ensure we residents have knowledge and a voice regarding future surveillance technologies. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used.
I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used. As a lifelong East Bay resident whose partner works in the City of Oakland, this is personal - I care what happens here and I want to see Oakland do the right thing.
It is absolutely crucial for Oakland to restore the trust of residents by bringing secret surveillance done by the City under control. Therefore, the provisions for a Standing Privacy Committee and safeguards regarding current and future surveillance systems be implemented ASAP!

I want to have documentation of activities in Oakland. I was recently robbed and it was a video set up by La Farine after a number of break ins and robberies that allowed my crime to be solved because a) the photos of both suspects was extremely clear as the crime was being committed; 2) the weapon used was clearly visible and added an enhancement for the crime; 3) the license plate number and the car's color and description allowed OPD to get a warrant for a tracking system for the vehicle which allowed OPD to solve more than just my crime. We need to be able to walk around Oakland without being suspicious of every person who matches the description of a suspect. We need to have criminals off the streets so that the city can move on to other quality of life issues and to make it more enjoyable for law-abiding citizens who pay taxes. With increased insurance costs, property taxes, wear and tear on the car because of the numerous potholes and poor roadways it costs 20% more to live in Oakland than it does to live in nearby Alameda.
Worried about side purchases new surveillance equipment by OPD/City Admin's office and apparent lack of input from the newly created privacy policy board and/or pre-purchase analysis of proposed purchases under City's privacy policy. ll are dangerous and will prove to be expensive.
I want to have a voice in the debate about surveillance and privacy in Oakland. I strongly urge you to accept Recommendation 7 from the ad hoc advisory committee on privacy to pass a citywide ordinance requiring public notice and debate before moving forward with new surveillance programs, legally enforceable privacy and retention policies, and oversight and accountability when technology is used.
Please put the breaks on surveillance. Constant surveillance is not appropriate in a democracy such as the United States.
Please protect our privacy Do not allow Oakland PD or any other law enforcement entity access to use our cell phones for location or any other reason other than to protect and serve us the citizens of the community We pay their Salaries and are Free Citizens of this Great Republic thank you
This center has no place in a democracy. Funds would be better spent on education for our children. The police as they are now, are a corrupt agency in desperate need of reform. We have the answers, lets not go forward in greed, fear and bigotry.
Stop it stop the 'them!'
I cannot express strongly enough how foolish it is for the Public Safety Committee to even consider approving a FLIR-outfitted helicopter without first completing a citywide privacy policy and making sure this new equipment is subject to it. It is not appropriate public policy to play bait and switch with the large public outpouring of opposition that met the Domain Awareness Center and resulted in the privacy policy development. Essentially this vote would be saying "it applies to this but not to that". That is reneging on the agreement made with the residents of the City that Oakland takes privacy seriously and will not proceed with aggressive surveillance until the rules of the privacy road are established. Please keep your word to the people of Oakland. Sincerely, Tracy Rosenberg, Media Alliance
Dear Oakland City Council, please don't squander this opportunity to enact a meaningful privacy and surveillance policy in Oakland to serve as a model for the rest of the country. I urge you to adopt the recommendations of the Privacy Advisory Committee.

Please make this happen. It is another tool for our understaffed police department to make the city safer using cameras that are already there. Please don't kow tow the loudest people at the council meeting. Do what is good for the majority of Oaklanders!!
I think that you need to implement the DAC. It is a great tool to prevent and fight crime. Please do not let a loud group of protesters deter you from doing what is right for the safety and well being of the city.
This looks entirely too restrictive. I'm worried that there might be a major disaster and our emergency services wouldn't be able to use this system.
This policy makes no mention of which data sources the DAC may consume, which is a disappointing omission. Early plans included data from all over Oakland, not merely "port adjacent" sources, and if that's still true, the Privacy Policy still doesn't seem to do enough to protect the privacy of Oakland's tax-paying citizens.
The privacy policy link isn't working....I can't offer input because I can't see the policy. :(
I support the privacy policy. I don't feel we should fund the DAC.
I am grateful for the work of the Privacy Policy and Advisory Committee. I am a lifelong Oakland resident eager to protect our community's privacy rights. I support the recommendations.
I support the Oakland Privacy Group. Do NOT fund the Domain Awareness Center. Why would you want to live in a police state?
Yes! Strict limitations on surveillance are necessary to protect privacy and prevent abuse.
Sounds creepy and unconstitutional
This 'survey' is a complete misnomer: There ought be no DAC. No amount of 'policies' will guard the privacy of Oakland's citizenry. Not only is city-wide surveillance WRONG . . . it's also UNCONSTITUTIONAL. THE CITY of OAKLAND will be SUED. Which is quite the fun irony; as Oakland does not possess the financial means to PAY for The DAC.
I have been following the progress of the Domain Awareness Center since it first hit publicly. I a fellow Californian strongly support all the "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. I support a standing privacy committee composed of outstanding public citizens Specific support for a surveillance equipment ordinance that doesn't encroach on person's right to privacy Specific support for penalties for wrongdoing.
I can see how spying on Oakland citizens might seem like a good idea on first blush. But please consider the long-term consequences of such surveillance before making this ill-judged investment.
As an Oakland resident and homeowner, I am deeply concerned about the implications of the DAC. I am writing to ask you to implement all of the Additional Recommendations, including a citywide privacy policy and a standing committee to oversee the activities of the DAC. As well, violations of DAC rules must be met with strict penalties - this is a power that would be very, very easy to abuse.

I strongly support all seven of the advisory committee recommendations, and submit the following additional points: 1. Strong support for all seven "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. 2. Specific support for a citywide privacy policy which could be used for this and future projects. 3. Specific support for a standing privacy committee which could propose additional recommendations and observe how the privacy policy is actually implemented. 4. Specific support for a surveillance equipment ordinance, which would prevent purchase of equipment which will ultimately used against our citizens rather than to protect them. 5. Specific support for penalties for wrongdoing and violation of the privacy policy so that the privacy policy can be enforced.
Hello. This is Tracy Rosenberg, executive director of Media Alliance, a democratic communications advocate located in Oakland. I am writing to encourage you to see the privacy package developed by the committee as a unified whole and as a model for a citywide policy. There is no doubt the City spoke up during the DAC process and said privacy is important to them. Supporting the whole package and extended it throughout the city is how the Council demonstrates a sincere response to the will of Oakland residents, which was overwhelmingly in support of limitations on surveillance. A standing privacy committee will allow Oakland to respond promptly and flexibly to new developments in technology, which as we know come fast and furious. Nothing about privacy and technology is static. The surveillance equipment ordinance is a crucial part of the package. Any and all technologies and equipment are subject to abuse and/or overreach and those kinds of problems occur when the rules of the road are not clear and where there is insufficient transparency. The ordinance provides a state of the art indemnification against both problems and will save Oakland a ton of money by preventing problems before they happen. Finally you should not be afraid to give the ordinance teeth with consequences for violations. This isn't punitive, its preventative. A policy with consequences is a policy that won't be disregarded too often and that is good for the residents of Oakland who won't be subject to random unfair or arbitrary privacy invasions and its good for the City of Oakland which will be sued far less often while modeling what the responsible use of surveillance looks like. Please support the privacy committee package in its entirety as a citywide privacy policy. Thank you for your consideration.
! very much support all the "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. In particular, I very much support a citywide privacy policy, a standing privacy committee, and especially a surveillance equipment ordinance. Finally it is ESSENTIAL that there be penalties for wrongdoing.
I recommend the adoption of the seven recommendations put forth by the Ad Hoc Advisory Committee. Can committees 1 & 5 be combined?
I strongly urge the adoption of the seven recommendations put forth by the Ad Hoc Advisory Committee, as well as: 1. Strong support for all seven "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. 2. Specific support for a citywide privacy policy which could be used for this and future projects. 3. Specific support for a standing privacy committee which could propose additional recommendations and observe how the privacy policy is actually implemented. 4. Specific support for a surveillance equipment ordinance, which would prevent purchase of equipment which will ultimately used against our citizens rather than to protect them. 5. Specific support for penalties for wrongdoing and violation of the privacy policy so that the privacy policy can be enforced.

I support and recommend the adoption of the seven recommendations put forth by the Ad Hoc Advisory Committee. In addition to the seven recommendations, I would like to see the following guidelines included: 1. Strong support for all seven "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. 2. Specific support for a citywide privacy policy which could be used for this and future projects. 3. Specific support for a standing privacy committee which could propose additional recommendations and observe how the privacy policy is actually implemented. 4. Specific support for a surveillance equipment ordinance, which would prevent purchase of equipment which will ultimately used against our citizens rather than to protect them. 5. Specific support for penalties for wrongdoing and violation of the privacy policy so that the privacy policy can be enforced.
I am in favor of strong privacy rights for all Oakland citizens. I strongly support the "additional recommendations." The DAC policy does not go far enough. I strongly support a citywide privacy policy and a standing privacy committee. I specifically support defining and enacting a surveillance equipment ordinance. Last, I strongly support penalties for wrongdoing. Regards, Thomas Ballantyne 3829 Webster St #1 Oakland, CA 94609
I fully agree with and support the Ad Hoc Committee's seven additonal recommendations. Without these I feel the Privacy Policy would not be effective. Additionally, I would like to see a citywide privacy policy which could be used for this and future projects. I would like a standing privacy committee which could propose additional recommendations and observe how the privacy policy is actually implemented. I would like a surveillance equipment ordinance, which would prevent purchase of equipment which will ultimately used against our citizens rather than to protect them. I would like to see penalties for wrongdoing and violation of the privacy policy so that the privacy policy can be enforced.
I strongly support all the "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. Additionally, I support a citywide privacy policy and a standing privacy committee. And I support a surveillance equipment ordinance, as well as penalties for wrongdoing. The already-precarious relationship between Oakland citizens and OPD will only be exacerbated by this spy center, and OPD doesn't need to incur the liability of a distrusting citizenry, and the City of Oakland can't afford the inevitable onslaught of civil rights lawsuits by DAC's true target--protestors! Thank you for considering my opinion.
I support the Advisory Committee recommendations, and offer strong support for all the "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope
Hello, I am a small business owner and resident in Oakland, and I strongly support all of the additional recommendations from the Advisory Committee. My business is in the data collection sector, and we disclose all of our methods of data collection and how we use the data. The city should do the the same. We must have a citywide privacy policy, privacy oversight committee, and stiff penalities for abusing data collected by the city. Additionally, mass surveillance equipment used by law enforcement should be considered illegal without a warrant. Data collection is very easy nowadays. However, we must be careful how we use that power. Having a strong privacy policy infrastructure and stopping the use of warrantless surveillance is a great step towards preserving the rule of law.

I strongly and unequivocably support the Privacy Committee's work. In particular, their recommendations for creating a city-wide privacy policy and a surveillance equipment ordinance are imperative in the world of ubiquitous governmental surveillance we have come to know that we live in. The people have a right to privacy, enshrined in the California Constitution but honored mostly in breach. The people have a right to be told of and make informed decisions about surveillance equipment. The City Council has an obligation to protect the civil liberties of its residents. Oakland can take important steps in this regard by enacting the Privacy Committee's recommendations in full. To be effective, to protect our rights, these provisions must have teeth - no one should be allowed to abuse these technologies and data for personal gain or in an effort to do an end-run around constitutional protections without knowing there is significant possibility of consequences. Destroying someone's life with information is no less consequential that impairing them by physical injury. Insofar as the DAC itself is concerned, it should never be brought online. It is neither desired, not needed, as the Port's refusal to fund it clearly illustrates. There are far better things to do to benefit Oakland with the money otherwise needed to operate and maintain it.
I strongly support all the additional recommendations, specifically that the privacy policy should be citywide, have a standing privacy committee, include a surveillance equipment ordinance with funding for oversight and enforcement. There must be penalties for wrongdoing; whenever a surveillance system is built, there will be abuse. The question is whether it's going to be discovered and remediated. Thank you for your concern.
1. I strongly support all of the "Additional Recommendations." These will have far more impact than the DAC Policy, which is too narrow in scope. 2. I specifically support a citywide privacy policy. 3. I specifically support a standing privacy committee. 4. I specifically support a surveillance equipment ordinance. 5. I specifically support penalties for wrongdoing. 6. The overall process of public involvement at the beginning, and transparency throughout, are also urgently needed.
1. I support all the "Additional Recommendations." 2. I support a citywide privacy policy. 3. I support a standing privacy committee. 4. I support a surveillance equipment ordinance. We must reverse our galloping course into Stasi world. 5. I support penalties for wrongdoing. Without them, there is no deterrence and will be abuse - as there is currently. I thank the Committee for its long, hard work. Susan Harman, Ed.D. Bay Area Civil Liberties Coalition CodePink Wellstone Democratic Renewal Club
I strongly support all the "Additional Recommendations." These will have far more impact than DAC Policy, which is too narrow in scope. I urge a citywide privacy policy. I believe there should be a standing privacy committee. There should be a surveillance equipment ordinance. There must be penalties for wrongdoing. If not, it gives carte blanche for all manner of corrupt and illegal behavior by those within the system.
I write to express strong support for a surveillance equipment ordinance. I agree with all the "Additional Recommendations" and their appropriate scope. I also strongly support a citywide privacy policy and a standing privacy committee. It also necessary to have penalties for wrongdoing. Overall, I believe it is essential to involve the public at the beginning of these processes and to maintain transparency throughout.

Dear Oakland City Council, I strongly support all the Additional Recommendations. I strongly support the city wide Privacy Policy. It is essential that it cover the whole city because it supports accountability. It is essential to have a standing committee on privacy to maintain citizen input on this critical issue. I support the surveillance equipment ordinance and penalties for wrongdoing. Regards, Kaliya, Identity Woman Independent Advocate for the Rights and Dignity of our Digital Selves.
I strongly support the recommendations of the DAC Advisory Committee. Although the DAC offers significant additional capability for the security of the Port of Oakland, it also creates numerous risks of violation of the civil rights of Oakland residents and visitors, in particular those related to the Fourth Amendment to the US Constitution. It should be assumed that these violations will occur unless prevented, given the recent history of similarly powerful data-gathering programs in other jurisdictions and at the national level. I urge the City of Oakland to adopt all of the Committee's additional recommendations as well as its proposed policy; they will offer meaningful protection against the civil-rights risks that come with the security capabilities of the DAC. Recommendation 3 in particular, which would make violation of the Policy a misdemeanor, is an important step to ensure that these protections are effective.
If people view this as "too creepy", less people will want to spend time in Oakland.
Restore the Fourth strongly supports the recommendations of the DAC Ad Hoc privacy committee. We especially support the adoption of strong penalties for wrong doing and whistleblower protections. We have seen in other communities like Seattle that strong privacy ordinances are ignored if no penalties are applied for ignoring them. The surveillance technologies being contemplated as part of the DAC and related technologies are just the tip of the iceberg in terms of what will be available to law enforcement in the near future. Oakland should lead the way in preserving the 1st Amendment rights essential to a free society from mass surveillance.
Please do not open the DAC. It is too intrusive and expensive. I would rather my taxpayer dollars be spent on opening libraries, fixing the streets, and providing services to youth and the poor. Please stop spying on us. Enough is enough. if you do open the DAC, please implement all of the suggestions made by this thoughtful committee. The public needs a say and oversight on mass surveillance.
Sounds okay, we want independent oversight over the program with plenty of input from the citizens. IMO: Many people are ignoring the dangers the city and port face because of the empowering of technology available at low cost to the individual and a turbulent international environment. Unlike many US cities, Oakland is a coastal city and that presents us with unique security challenges. The port of Oakland can help provide prosperity to California and this region. Prudent security will help us to compete among many nations, and security threats. We do not need to give up our liberty to protect our city.
I fully support having this privacy policy for the DAC. I believe any surveillance equipment installed by the city of Oakland should have to follow this policy or something similar. I think Shotspotter, LPR, and stingrays are far too intrusive to be given a 'free' ride.

Attachment B

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

I. BACKGROUND AND OVERVIEW

The 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 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.

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 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.

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 decisions 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. The 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~~ 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~~ 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 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~~ Center will only be implemented in a ~~port~~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 the PSIM system that allows staff to mark and annotate data for later review; the time stamped record is the bookmark.

"Compliance Officer" An employee whose responsibilities include ensuring that the organization complies with its internal policies and outside regulatory requirements.~~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 Staff" means the City of Oakland employees who will be 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 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

Forma (Defau Roman
Forma (Defau Roman
Forma (Defau Roman

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."

The Chief Privacy Officer (CPO) is a senior level administrator within the City of Oakland 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 the staff are kept up-to-date with changes, if any, in 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. ~~"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~~ 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 ~~Record Keeping and Auditing~~Recordkeeping 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, 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 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 DAC Staff and DAC Vendors.

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 levels and will be required to sign binding Non-Disclosure Agreements to ensure data and information security.

Training

Training by the ~~Internal~~ 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.

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 Department Directors, Mayor, City Council Members, 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 DAC Vendors that installed the systems as well as other maintenance providers will have access to the system components 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.

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, 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 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 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~~ Chief Privacy Officer no later than 8 hours after activation of the DAC System.

IX. INTERNAL CONTROLS, AUDITS AND REPORTING METRICS

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.

~~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

~~**Internal Recordkeeping, Auditing, and Internal Privacy Officer**~~

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 limited to, 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).

Chief Privacy Officer

It is recommended that a City manager or designee be assigned to serve as **Chief Privacy Officer**. The Chief Privacy Officer (CPO) is a senior level administrator within the City of Oakland who is responsible for managing the risks and business impacts of privacy laws and policies. The CPO will be charged with ensuring the DAC staff is kept up-to-date with changes, if any, in policies and procedures related to privacy for the DAC functions, to include City measures or other legislative measures, and will oversee any training required to maintain compliance.

~~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).~~

Chief Compliance Officer

The Chief Compliance Officer is an employee whose responsibilities include ensuring that functions related to the DAC ~~complies~~comply with the DAC 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 following areas within the DAC function:

~~**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~~

Forma
Times
pt

Forma
No bull

~~information and describe any corrective action taken or needed:~~

1. ~~**Purpose Specification**~~**DAC System Usage**: ~~General statistical breakdown of~~An overview of how the DAC System ~~was~~ is used including:
    a. ~~Listing and number of incident~~ Incident records by incident category
    b. ~~Average time tot~~Timing required to close an incident record
    c. ~~a~~Actionable events, non-actionable events, and false alarms. ~~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~~is meeting its stated purpose, to ~~,~~ include a review and assessment of ~~ing:~~
    a. Crime statistics for geographic areas where the DAC was used;
    b. The ~~number of times the~~frequency in which DAC was used to bookmark or retain data for potential criminal investigations;
    c. The ~~number of times~~occurrences in which DAC Data was shared for potential criminal investigations;
    d. Lives saved;
    e. Incidents in which assistance was provided to ~~P~~persons, property, land and Natural Habitat security, ~~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 summary of how the DAC data is shared with other non-City entities, to include a review and assessment of
    a. The type of data disclosed;
    b. Justification for disclosure (e.g., warrant, memoranda of understanding, etc.)
    c. The recipient of the data;
    d. Dates and times 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 VIIIA 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?~~A reporting of the incidents, ~~(~~if any~~)~~, of disclosure of DAC Data that do not comply with DAC policy, follow-up procedures, resolutions and consequences.
5. **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, evidence of written certifications, follow-up procedures, resolutions, and consequences. ~~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, as required or permitted by the City's Whistleblower program.
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, 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.

8. **Data Retention:** A summary of the data retained within the DAC process and an assessment of compliance to the Data Retention requirements as stated in the DAC policy. ~~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.~~The process to provide access and specific permission levels to authorized persons/staff working in the DAC function.
10. **Public Access:** ~~Statistics and information about public records requests received, including response rates.~~A summary of the public records requests received, responses, and an evaluation of the appropriateness of records submitted and timeliness of responses.
~~11. **Cost:** Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs.~~

~~Independent Audits~~ Internal Control Reviews and Audits

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.

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 ~~for this area. 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.~~

~~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.~~

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:

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 Auditing, External Audits,~~ 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 ~~in January~~at a designated timing ~~of~~ each year~~,~~

~~or at the next closest regularly scheduled council meeting~~. The City Council should use the Report and the information ~~it's~~ it is 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 comply with all relevant and applicable Data Retention policies and 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.

Attachment C

CITY OF OAKLAND

ONE FRANK H. OGAWA PLAZA • ELEVENTH FLOOR • OAKLAND, CALIFORNIA 94612

Public Ethics Commission

(510) 238-3593
FAX (510) 238-3315
TDD (510) 238-3254

April 6, 2015

President McElhaney and Council Members
Oakland City Council
1 Frank Ogawa Plaza
Oakland, CA 94612

Dear President McElhaney and Council Members,

At its public meeting on March 2, 2015, the Public Ethics Commission (Commission) reviewed and discussed the Privacy and Data Retention Policy developed by the Domain Awareness Center Ad Hoc Advisory Committee, as well as the companion recommendations in the related Agenda Report Memorandum dated January 28, 2015. This letter communicates the Commission's concerns regarding the proposed Policy and recommendations.

The recommendations outlined in the Agenda Report include a role for the Public Ethics Commission to "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."

In discussions about the proposal, the Commission articulated a number of concerns regarding the proposed role for the Commission. First, the Policy crosses a number of federal, state, and local laws regarding privacy, civil rights, freedom of speech, freedom of information, and whistleblower protection, many of which would be new areas of law and jurisdiction for the Commission. Second, the Commission just received authorization of additional staff positions in November 2014 that aim to fill a gap in Commission resources that had existed for many years, as well as the expansion of its jurisdiction by way of an entirely new and complex ordinance: the Government Ethics Act. The Commission now is focused on making these staffing and jurisdictional changes and is not presently equipped to take on another complex set of laws and accompanying legal jurisdiction.

The Commission will continue to monitor the progress of the proposed DAC policy and will continue to provide information to the advisory committee as needed. Meanwhile, the Commission has not taken a formal position on the policy; however, Commissioners expressed the above concerns about Commission resources, jurisdiction, and capacity as it relates to the proposed role for the Public Ethics Commission.

This letter was approved by the Public Ethics Commission at its meeting on April 6, 2015.

Sincerely,

Jenna Whitman
Public Ethics Commission Chairman, on behalf of the Commission

Attachment A

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

I. BACKGROUND AND OVERVIEW

The 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 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.

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 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.

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 protect 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 decisions 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. The 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 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 City Council 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 only 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 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.

"Chief Privacy Officer" (CPO) is a senior level administrator within the City of Oakland 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 the staff are kept up-to-date with changes, if any, in 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.

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

"Compliance Officer" An employee whose responsibilities include ensuring that the organization complies with its internal policies and outside regulatory requirements.

"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" means the City of Oakland employees who will be 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.

"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 DAC Staff and DAC Vendors.

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 levels and will be required to sign binding Non-Disclosure Agreements to ensure data and information security.

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.

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 Department Directors, Mayor, City Council Members, 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 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.

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, 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 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
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.

IX. INTERNAL CONTROLS, AUDITS AND REPORTING METRICS

Chief Privacy Officer

It is recommended that a City manager or designee be assigned to serve as Chief Privacy Officer. The Chief Privacy Officer (CPO) is a senior level administrator within the City of Oakland who is responsible for managing the risks and business impacts of privacy laws and policies. The CPO will be charged with ensuring the DAC staff is kept up-to-date with changes, if any, in policies and procedures related to privacy for the DAC functions, to include City measures or other legislative measures, and will oversee any training required to maintain compliance.

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.

Compliance Officer

The Chief Compliance Officer is an employee whose responsibilities include ensuring that functions related to the DAC 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 following areas within the DAC function:

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.

Internal Control Reviews and Audits

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.

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:

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.

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 comply with all relevant and applicable Data Retention policies and 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.

Approved as to Form and Legality

City Attorney

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2015 APR 30 PM 4:11

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 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 attached "Policy for Privacy and Data Retention for the Port Domain Awareness Center (DAC)" as City 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