CITY OF OAKLAND
POLICY FOR PRIVACY AND DATA RETENTION FOR THE PORT DOMAIN AWARENESS CENTER (DAC)

I. BACKGROUND AND OVERVIEW

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

Under this grant program, funding was available for Maritime Domain Awareness (MDA) projects relative to "maritime" or "waterside". 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 clearly limited the scope of the DAC to the Port. Therefore, the DAC and the entirety of this policy are exclusive to Port areas within Oakland. 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). 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.

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 and erect safeguards around any data captured and retained by the DAC, and to protect against its improper use, distribution and/or breach. This policy shall be referred to as the DAC Privacy and Data Retention Policy ("Policy"). More specifically, the principal 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.

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 as a consequence of participating in modern society.

IV. UPDATES TO THE POLICY AND TO DAC

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

B. The Oakland City Council has placed limits on current and future technology for the DAC. Specifically, Oakland City Council Resolution 84593 provides in relevant part, the following:

"The Domain Awareness Center (DAC) Phases 1 and 2 includes data and video feeds from the following surveillance, security sensor and video analytics sources only: Port Video and Intrusion Detection Cameras, Port of Oakland Vessel Tracking System, City of Oakland Shot Spotter Audio Sensor System (only those sensors that provide coverage to Port areas). The addition of any new surveillance, security sensor or video analytics capability, feed or data sources shall require approval of the Council, including confirmation of compliance by the DAC and all City and Port data sources with the City's Privacy and Data Retention Policy to the extent allowed by law."

V. DEFINITIONS

As used in this Policy framework, 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.

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

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

"DAC Data" means any data or information fed or stored into the DAC System, or derived therefrom, or work product of the DAC Staff.

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

"DAC Staff" means the City of Oakland employees who will be responsible for monitoring the equipment within the DAC on a day-to-day basis, including supervisors, and that have completed appropriate training prior to interaction with the DAC.

"DAC System" means 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), Fire Automatic Vehicle Location (Phase 2), NOAA Weather Alerts (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.

"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 Port DAC systems, data, and staff.

“Internal Privacy Officer” means the EOC Manager who is charged with ensuring the DAC Staff are abiding by the 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.

“Major Emergency” means the existence of conditions of disaster or extreme peril to the safety of persons and property within the territorial limits of the Port of Oakland or having a significant adverse impact within the territorial limits of the Port of Oakland, caused by such conditions as air pollution, fire, flood, storm, epidemic, drought, sudden and severe energy shortage, plant or animal infestation or disease, the state Governor’s warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, which are likely to be beyond the control of the services, personnel, equipment, and facilities of the City of Oakland and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the California Public Utilities Commission.

“Need to know” means even if one has all the necessary official approvals (such as a security clearance) to access the DAC System, one shall not be given access to the system or DAC Data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the allowable uses in Section VIII of this Policy. Furthermore, the “need” shall be established prior to access being granted.

“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), name, social security number, physical description, home address, telephone number, other telephone identifiers, education, financial matters, medical history, employment history, photographs of faces, movements, distinguishing marks, license plates, cellphone meta-data, internet connection meta-data. There is a strong, definitive relationship between Personal Identifiable Information and the individual in that Personal Identifiable Information (PII) belongs to the individual (is considered their property) and is his/hers to disclose or to keep private to himself.

“Protected Activity” means all rights including without limitation: speech, associations, conduct, and privacy rights protected by the United States Constitution and/or the California Constitution and/or applicable statutes and regulations including but not limited to expression, advocacy, association, or participation in expressive conduct to further any political or social opinion or religious belief. Advocacy of the use of force or law violation is lawful Protected Activity, except where such advocacy is directed to inciting or producing imminent unlawful violent action and is likely to incite or produce such an action.

- Example: John Smith, age 18, has 1 Twitter follower and a public Twitter account. On Twitter, he announces he will be attending tomorrow's "FTP" rally to "wreak havoc." John Smith has no previous criminal history, and OPD has never heard of him. It is unlikely John Smith will engage in violent conduct, and use of the DAC System would likely not be warranted under these circumstances.
- Example: Via public posts from well organized groups on social media asking attendees at an Urban Shield protest to bring bolt cutters, gas masks, and baseball bats to tomorrow's rally, and because some of the posting members have previous violent criminal records from arrests in the City of Oakland, DAC Staff would likely be able to argue that activation of the DAC System to monitor the rally, a form of Protected Activity, is reasonable under the circumstances present.

"Reasonable Suspicion" means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise. Reasonable Suspicion shall not be based on Protected Activity. Furthermore, a suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

"Right to Privacy" means 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 further understood when one divides privacy into three equally significant parts: 1) Secrecy - our ability to keep our opinions known only to those we intent 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, where the message might not be secret at all - Anonymity is the only protection against retaliation for opinions or whistleblowing. 3) Autonomy - Ability to make our own life decision free from any force that has violated our secrecy or anonymity.

VI. ACCESS TO THE DAC SYSTEM / EQUIPMENT

Day to Day Operations

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

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

Training

Training 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 with EOC activation, notwithstanding the Memorandum of Understanding requirements in section VII, City of Oakland Agency Directors and/or their designees in the Emergency Operations Center (EOC) and outside governmental agencies and non-governmental agencies' staff assisting with the Allowable Use or disaster (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 or disaster and DAC operations.

Support and Repairs

ITD staff and vendors that installed the systems as well as other maintenance providers will have access to the system components but will be prohibited from access to DAC data. Various manufacturers and vendors are hired to provide additional support services. Any system and network level access by these vendors require both a background check and ITD employee presence. The system level access is maintained by ITD staff, however the Applications level access, as far as end-users are concerned, is maintained by the DAC Staff.

Funding Auditing Purposes

Federal, State, or Local funding auditors or the City Auditor 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

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

In order for DAC Staff to provide DAC Data to non-City of Oakland agencies there must be a warrant based upon probable cause or a written MOU that is approved by the City Council after enactment of this policy. Additionally, 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.

The DAC shall not record any data except bookmarks of Allowable Uses as defined in Section VIII.

VIII. USE AND EXCEPTIONS

A. Uses: The following situations at the Port are the only ones in which the use of the DAC is allowable:

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
Heat Wave
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. Exceptions: 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 Privacy Officer no later than 8 hours after initiation of the DAC system.

IX. AUDITS AND REPORTING METRICS

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

Internal Recordkeeping and Auditing

DAC Staff shall keep records sufficient 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).

The Internal Privacy Officer 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.

External Audits

Quarterly and as needed audits of the DAC System will be conducted and made publicly available by the Compliance Officer to ensure compliance with this Policy. The audit shall include the following and describe any corrective action taken or needed:

1. **Purpose Specification**: General statistical breakdown of how the DAC System was used including:
    a. Listing and number of incident records by incident category
    b. Average time to close an incident record
    c. Number of incidents actionable by DAC Staff vs. number of incidents non-actionable and/or false alarms.
2. **Public Safety Effectiveness:** Information and conclusions about whether the DAC has accomplished its stated purpose, including:
    a. Crime statistics for geographic areas where the DAC was used;
    b. The number of times the DAC was used to bookmark or retain data for potential criminal investigations;
    c. The number of times DAC Data was shared for potential criminal investigations; and
    d. Criminal charges brought using evidence derived from use of the DAC System or DAC Data.
3. **Data Sharing:** How many times DAC Data was shared with non-City entities and:
    a. The type of data disclosed;
    b. Justification for disclosure (e.g., warrant, memoranda of understanding, etc.)
    c. The recipient of the data;
    d. Date and time of disclosure; and
    e. Obligations imposed on the recipient of shared information.
4. **Data Minimization:** Describe whether and how the DAC System was used in a manner not allowed under Section VIII of this Policy. Describe whether and how the DAC Data was accessed in violation of this Policy. What were the consequences of such misuse?

5. **Protected Activity Exception:** The number of times DAC Staff certified use of the Protected Activity Exception as provided in Section VIII B, and copies of each written certification.
6. **Dispute Resolution:** Description of the number and nature of complaints filed by citizens or whistleblowers and the resolution of each.
7. **Requests for Change**: A summary of all requests made to the City Council for approval of the acquisition of additional equipment, software, data, or personnel services including whether the City approved or rejected the proposal and/or required changes to this Policy before approval.
8. **Data Retention:** Describe whether data was retained in violation of this Policy.
9. **System Access Rights Audit**: Verification that individual user assigned access rights match access rights policy for user's designated staff role.
10. **Public Access:** Statistics and information about public records requests received, including response rates.
11. **Cost Justification:** Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs.

Independent Audits

The City Council shall provide for annual independent third party audits of DAC performance and security. The auditor shall have full access to Internal Recordkeeping, the DAC System, and the DAC Data. The results of the independent audit shall be made publicly available.

Annual Report

The Compliance Officer shall prepare and present an Annual Report that summarizes and includes the results of **Internal Recordkeeping and Auditing, External Audits, and Independent Audits,** and present it to the City Council at a public meeting in January of each year, or at the next closest regularly scheduled council meeting. The City Council should use the Report and the information it's based on to publically reassess whether the DAC benefits outweigh the fiscal and civil liberties costs.

X. RECORDS MANAGEMENT

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

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

XI. REDRESS AND PUBLIC INFORMATION REQUESTS

To the extent the request is not in conflict with applicable California or Oakland 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

Any Person found guilty of knowingly or willingly 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. Any violation of any section of this Policy is an injury of persons affected by such violation.

Any Person who knowingly or willingly violates any section or provision of this Policy 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. Therefore this Policy defines violations of the privacy and retention Policy as an injury to persons affected by such violations.

Violations of this Policy shall result in consequences that may include retraining, suspension, termination, 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.