

Kate Harrison  
Councilmember District 4

## REVISED AGENDA MATERIAL for Supplemental Packet 1

**Meeting Date:** July 26, 2022

**Item Number:** 29

**Item Description:** Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers

**Submitted by:** Vice Mayor Harrison

### **RECOMMENDATION**

Adopt the updated BPD Policy 1302, the legally enforceable Surveillance Use Policy for Automated License Plate Readers (ALPR) pursuant to BMC 2.99.

### **BACKGROUND**

The proposed Policy 1302 represents near complete agreement between BPD, the City Manager's Office, and Vice Mayor Harrison's Office.

Council originally financed and authorized ALPR technology to help automate BPD's parking and scofflaw enforcement, but through BPD policy development, usage expanded to criminal enforcement. To date, due to the pandemic and policy concerns regarding data retention, sharing, and civil liberties protections, Council deferred adoption of a Surveillance Use Policy pursuant to BMC Sections 2.99.020 and 2.99.050 of the Surveillance Ordinance for ALPR.

BPD Administrative Order #001-2016, prepared in 2016 before adoption of the Surveillance Ordinance, has served as a de facto ALPR policy, yet Administrative Order #001-2016 is out of date with local and state law and does not satisfy the specific requirements of the Surveillance Ordinance. Most recently, adoption of a proposed update to the use policy for ALPRs (Policy 1302) was deferred by Council in 2020 and 2021. In November 2021, Councilmembers Harrison and Hahn, and separately Councilmember Taplin, submitted proposed revisions. Council referred the matter to the Agenda Committee for future scheduling to allow for further policy development.

Since the referral to the Agenda Committee, Vice Mayor Harrison and Councilmember Hahn have been working diligently with BPD, the City Manager, City Attorney, the Information Technology and Public Works Departments, and City Contractors to craft a sensible policy that (1) fully addresses the requirements of the Surveillance Ordinance, (2) clarifies the purpose and scope of collection, (3) enacts various safeguards to protect sensitive data, and (4) provides clarity on the circumstances when parking enforcement and analysis ALPRs and associated data can be used to support criminal investigations.

Use Policy Updates Overview:

*Definitions*

- Provides key new definitions related to the City's ALPR equipment, vendors, and data types. Also provides definitions for Parking Enforcement Operations and Parking Analysis as part of the goBerkeley system.
- Enumerates the specific authorized uses of ALPR technology associated with Parking Enforcement and Parking Analysis.

*Authorized and Prohibited Uses*

- Allows BPD to query ALPR data retroactively to support a specific BPD criminal investigation when an officer has a good faith belief that an emergency involving the danger of, or imminent threat of death or serious physical injury to any person requires such a query or use, and the officer reasonably believes there is a nexus between a vehicle and the alleged crime scene. Approval to query the data must be granted by the Chief of Police and City Manager. The City Manager shall log any queries or use of such information pursuant to this subsection in its Annual Surveillance Technology Report pursuant to BMC 2.99.
- Provides that officers may investigate hits based on reasonable suspicion resulting from apparent matches, discovered in the regular course of work of Parking Enforcement Operations, between the Genetec ALPR System and the following databases: Stolen Vehicles System, Amber, Silver, and Blue Alerts, local missing persons, scoff law violator, gig car, general permit, or other non-criminal local lists.
- Explicitly prohibits ALPR use that invades privacy and during crowd control.
- Limits the use of ALPR in conjunction with lists or databases to the: Stolen Vehicles System, Amber, Silver and Blue Alerts, local missing persons, scoff law violator, gig car, general permit, or other non-criminal local lists.

*Data Collection and Retention*

- *ALPR Reads Not Resulting in ALPR Hits* - All ALPR Read Images and ALPR Read Metadata transmitted to and stored in the Genetec ALPR System shall be purged within fourteen (14) days to allow for the City's enforcement of its

72- Hour Rule (BMC Section 14.36.050).

ALPR Read Metadata in the form of license plate data or other non-PII data may be transmitted to and stored in the Passport Automatic Data Collection System for Parking Analysis purposes and retained pursuant to applicable retention policies.

- *ALPR Hits* - All ALPR Hits and related metadata resulting from ALPR Reads should be uploaded daily to the Genetec server and shall be purged from Genetec within fourteen (14) days to allow for the City's enforcement of its 72-Hour Rule (BMC Section 14.36.050).
- *Unenforced ALPR Hits* - All erroneous and unenforced ALPR Hit data shall be purged locally at least nightly.
- *Enforced ALPR Hits* - Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management System servers, with a maximum retention period of one (1) year in Passport and in accordance with the established records retention schedule.

#### *Third Party Data Sharing*

- The ALPR data may be shared only with other law enforcement or prosecutorial agencies as pursuant to a valid court order, subpoena, or a search warrant, Cal. Civ. Code §1798.90.5(f), and as limited by this Policy, and shall not be shared with federal immigration enforcement officials consistent with this policy and other applicable City policy.
- Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided by this policy and the Records Maintenance and Release Policy.
- Aggregated ALPR data not related to specific criminal or civil investigations authorized by a court order, subpoena, or search warrant shall not be released to any local, or state agency or entity without the express written consent of the City Manager and only in accordance with this Use Policy.



# **Surveillance Use Policy --ALPR- Automated License Plate Reader**

## **1302.1 PURPOSE**

This Surveillance Use Policy is ~~issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by legally-enforceable pursuant to~~ BMC 2.99.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for Parking Enforcement Operations, Parking Analysis, and limited criminal enforcement purposes associated with Parking Enforcement Operations while recognizing the established privacy rights of the public.

## **1302.2 DEFINITIONS**

"Alleged Parking Violation" means an alleged violation of time limits in parking areas designated by state and local law, or a violation of time limits and/or non-permit parking in the City's RPP zones.

"ALPR Read Image" means images of license plates, vehicles, wheels or any other incidentally captured image.

"ALPR Read" means computer-readable data captured by an ALPR Reader, including ALPR Read Image and associated ALPR Read Metadata. ALPR Reads are transient means to create potential government records, to include Parking Analysis data and Enforced Citations.

"ALPR Hit" means an Alleged Parking Violation or Stolen Vehicle System alert resulting from computer generated analysis of ALPR Reads by the Genetec ALPR System resulting in an apparent:

1. match between an ALPR Read and ALPR Read Metadata stored in the Genetec ALPR System, to include the Stolen Vehicle System; or
2. cross checking between ALPR Read and permit information which is stored on the Genetec ALPR System.

"ALPR Read Metadata" means any image-based or other metadata, including but not limited to, global positioning system coordinates, block face information, tire position information, digitized license plates in alphanumeric characters, and timestamps.

"Automated License Plate Reader" or "ALPR" means one or more Genetec AutoVu mobile cameras affixed to Parking Enforcement Vehicles and combined with computer software and algorithms to read and convert images of license plates, the characters they contain, and associated ALPR Read Metadata related to Parking Enforcement Operations or Parking Analysis into computer-readable data.

"Deploy" or "Deployment" means any operation or use of ALPR Readers affixed to Parking Enforcement Vehicles.

"Enforced ALPR Hit" means an Alleged Parking Violation confirmed by a Parking Enforcement



Officer that results in the transmission of associated ALPR Read Image and ALPR Read Metadata to the Passport Parking Management System for storage in a database as a government record for the purpose of citation processing.

"Genetec ALPR System" means the computerized Genetec server and database that stores all ALPR Reads, metadata and hits, and also pushes an Enforced ALPR Hit metadata to the Passport Parking Management System.

"Residential Parking Permits" or "RPP" means an annual, visitor, merchant or in-home care parking permit, typically represented by a vehicle's license plate, and associated with the City's Residential Parking Permit program across designated zones.

"Parking Enforcement Vehicle" means the GO-4 three-wheeled parking enforcement vehicle.

"Parking Enforcement Officers" means employees of the City who work weekly rotations on Parking Enforcement Operations beats throughout the City and are properly trained to operate ALPRs and access the Genetec ALPR System.

"Parking Enforcement Operations" means Parking Enforcement Officer enforcement of parking regulations associated with local ordinances, the California Vehicle Code, and Stolen Vehicle System enforcement through Parking Enforcement Vehicle-based automated (ALPR) and non-automated means.

"Personally Identifiable Information" or "PII" means information:

1. that directly identifies an individual (e.g., name, address, telephone number, email address, etc.) or
2. by which the City or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

"Parking Analysis" means ongoing computational or algorithmic analyses performed by the City of Berkeley on ALPR Read Metadata regarding the occupancy of total parking spaces across commercial districts as part of goBerkeley, the City's data-driven, demand-responsive parking management program. ALPR Read Metadata data associated with Parking Analysis may include non-randomized license plates, to be maintained by Public Works for Parking Analysis.

"Parking Permit Application" means an application submitted to the City for RPP or other permit that may include but is not limited to PII such as names, address, photo identification, vehicle registration (license plate and vehicle identification number), phone number and email address.

"Passport Automatic Data Collection System" means the server and database whereby the Passport Parking Management System vendor, on behalf of the City, downloads, stores and transfers Parking Analysis ALPR Read Metadata stripped of any and all PII before being transferred to the goBerkeley program.

"Passport Parking Management System" means the servers and databases maintained by Passport Labs Incorporated, containing the database of the license plate numbers and other PII associated with Parking Permit Applications and Residential Parking Permits, and including historic parking citation data, to include Enforced Hits.

"OPSMAN Mobile" means a mobile device providing handheld ticket issuance and ALPR data reference capabilities.

"Stolen Vehicle System" or "SVS" means information from the California Law Enforcement Telecommunications System's (CLETS) Department of Justice (DOJ) Stolen Vehicle System (SVS) database providing data regarding wanted and stolen vehicles.

### **1302.3 AUTHORIZED AND PROHIBITED USES**

Use of an ALPR is restricted to the purposes outlined below.

All data and images gathered by the ALPR are for ~~the~~ official use ~~of~~ by the Berkeley Police Department (BPD) for Parking Enforcement Operations and may be retroactively queried in limited circumstances only as specified by this department. Because such data may contain policy and/or federal, state, local law.

ALPR data may be used by the Finance, Information Technology (IT), Customer Service, and Public Works Departments only as specified in this policy, and consistent with Parking Enforcement Operations and Parking Analysis. Data that is considered confidential information, pursuant to case law, state statutes, and BPD Policy 804 Records Release Management and/or applicable federal, state, or local law is not open to public review. (Ref. policy 422.2)

Berkeley Police

## ~~1302.2~~ AUTHORIZED AND PROHIBITED USES

~~Use of an ALPR is restricted to the purposes outlined below.~~ Department members or other Departments shall not use, or allow others to use the equipment or database records for any unauthorized purpose ~~(Civil Code § 1798.90.51; Civil Code § 1798.90.53). (Ref. policy 422.4),~~ and will enforce this policy pursuant to Section 1302.11(1).

- (a) An ALPR shall only be Deployed and used for official law enforcement business Parking Enforcement Operations, and Parking Analysis.
- (b) ALPR data obtained from Parking Enforcement Operations and retained pursuant to this use policy, including data and metadata associated with ALPR Reads and Hits, may be queried and used to support a specific BPD criminal investigation when an officer has a good faith belief that an emergency involving the danger of, or imminent threat of death or serious physical injury to any person requires such a query or use, and the officer reasonably believes there is a nexus between a vehicle and the alleged crime scene. Approval to query or use the data must be granted by the Chief of Police and City Manager. The City Manager shall log any queries or use of such information pursuant to this subsection in its Annual Surveillance Technology Report pursuant to BMC 2.99.
- (c) Notwithstanding subsection (b), officers may investigate hits based on reasonable suspicion resulting from apparent matches, discovered in the regular course of work of Parking Enforcement Operations, between the Genetec ALPR System and the following databases: Stolen Vehicles System, Amber, Silver, and Blue Alerts, local missing persons, scoff law violator, gig car, general permit, or other non-criminal local lists.
- (d) Data obtained from Parking Analysis shall not be queried or used for criminal investigations.
- (e) The following uses of the Genetec ALPR System are specifically prohibited:

### 1. Invasion of Privacy

- (a) It is a violation of this Policy to utilize the Genetec ALPR System to capture license plates not on a public road or street, or in a place not accessible to the public.

### 2. Crowd Control

- (a) ALPRs shall not be deployed in crowd control operations except strictly for the purposes of Parking Enforcement Operations.

### 3. Criminal Enforcement

- (a) It is a violation of this Policy to use or Deploy ALPRs to scan or canvass license plates in connection with any crime scene, patrol operation, or investigation except pursuant to Section 1302.3(c) of this Policy.

### 4. Use of Lists and Databases

- (a) It is a violation of this Policy to use the Genetec ALPR System or

associated ALPR Read data in conjunction with any list or database other than those specified pursuant to Section 1302.3(c) of this Policy, or for any personal use.

~~1302.4~~ An ALPR may be used to support a patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

~~(a) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.~~

### ~~1302.3 DATA COLLECTION~~

~~All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may~~ **DATA COLLECTION AND RETENTION**

The Investigations Division Captain, or their designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT) Department and associated Genetec ALPR system providers/vendors as identified below.

IT's role will be limited to providing initial infrastructure set-up and accessing or viewing individual records or reports (potentially including PII or CLETS information as authorized by the Chief of Police), and testing the accuracy of the equipment. Genetec ALPR System data provided to Parking Control Officers may also contain confidential CLETS information and is not open to public review.

~~(a) ALPR information gathered and retained by this department may be used~~ Read Images

ALPR Reads Images are license plate images which are uploaded daily Genetec server and shall be purged pursuant to the retention guidelines in subsection (b).

~~(b) ALPR Reads Not Resulting in ALPR Hits~~

All ALPR Read Images and shared with prosecutors ALPR Read Metadata transmitted to and stored in the Genetec ALPR System shall be purged within fourteen (14) days to allow for the City's enforcement of its 72- Hour Rule (BMC Section 14.36.050).

ALPR Read Metadata in the form of license plate data or other non-PII data may be transmitted to and stored in the Passport Automatic Data Collection System for Parking Analysis purposes and retained pursuant to applicable retention policies.

~~(c) ALPR Hits~~

All ALPR lawHits and related metadata resulting from ALPR Reads should be uploaded daily to the Genetec server and shall be purged from Genetec within fourteen (14) days to allow for the City's enforcement agencies only as permitted by law. (Ref. policy 422 of its 72-Hour Rule (BMC Section 14.36.050).

~~(d) Unenforced ALPR Hits~~

All erroneous and unenforced ALPR Hit data shall be purged locally at least nightly.

~~(e) Enforced ALPR Hits~~

Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management System servers, with a maximum retention period of one (1) year in Passport and in accordance with the established records retention schedule.

1302.5 }

#### ~~1302.4~~ DATA ACCESS

- (a) Only properly trained Parking Enforcement Officers, Sworn Officers as selected by the Investigation's Division Captain, and Information Technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information.
- ~~(a)~~(b) No member of ~~this department~~the BPD shall operate ALPR equipment or access ALPR data without first completing department-approved training, which shall include compliance with this use policy.
- ~~(b)~~(c) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- ~~(c)~~(d) If a Sworn officer is called to verify a stolen vehicle, if practicable, the officer should verify an ALPR response through ~~the California Law Enforcement Telecommunications System (CLETS)~~ before taking enforcement action that is based solely on an ALPR ~~alert~~Hit.
- (e) Sworn Officers shall visually verify that the license plate of interest matches identically with the ALPR Read Image of the license plate number captured (ALPR Read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. BPD members alerted to the fact that an observed motor vehicle's license plate is entered as an ALPR Hit in a specific Stolen Vehicle System list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

1302.

**1302.5 — 6 DATA PROTECTION**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data ~~(Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.6):~~

- (a) All ALPR data downloaded to any workstation or server shall be accessible only through a login and/or password-protected system capable of documenting all access of information by name, date and time ~~(Civil Code § 1798.90.52).~~
- (b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for ~~legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.~~ Parking Enforcement Operations or

~~Aggregated ALPR data not related to specific BPD criminal or civil investigations shall not be released to any local, state or federal agency authorized by a court order, subpoena, or entity without the express written consent of the City Manager search warrant.~~

- (c) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question. If a Berkeley Police Department member becomes aware of an inaccurate manual entry into the ALPR databases, that member shall immediately contact the originating agency or officer to notify the agency of the inaccuracy. The member shall then notify both the Investigations Division Captain and the Inspections and Audit Sergeant of the data error for appropriate follow up and tracking.

**1302.67 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal, state, and ~~state~~local law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third-Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to impacts that may violate the First and Fourth Amendments and other potentially disparate or adverse impacts on any communities or groups.

**1302.7 — DATA RETENTION**

~~The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT) department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records. The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for the purpose of federal immigration~~

enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

~~All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)~~

~~(-) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.~~

### 1302.8 PUBLIC ACCESS

~~(a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. (Ref. policy 422.6 (a))~~

Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of ~~his or her~~their identity and of ownership of the vehicle in question. ~~(Ref. policy 422.6 (b))~~All requests will be evaluated on a case-by-case basis to ensure they conform to the requirements and limitations of public records requests and other applicable law.

### 1302.9 THIRD -PARTY DATA-SHARING

(a) Non-law enforcement requests for anonymized ALPR bulk data related to parking enforcement and access to stored ALPR data related to parking management shall be processed according to this policy, the Records Maintenance and Release Policy and applicable federal, state, and local law.

~~(a)(b)~~ The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes as pursuant to a valid court order, subpoena, or as otherwise a search warrant, Cal. Civ. Code § 1798.90.55(b), and as permitted by law. ALPR data is subject to the provisions of BPD Policy 415, and hence may this policy and shall not be shared with federal immigration enforcement officials consistent with this policy and other applicable City policy.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in by this policy and the Records Maintenance and Release Policy ~~(Civil Code § 1798.90.55).~~

Aggregated ALPR data not related to specific criminal or civil investigations authorized by a court



order, subpoena, or search warrant shall not be released to any local, ~~or state or federal~~ agency or entity without the express written consent of the City Manager. ~~(Ref. policy 422.6 (e))~~ and only in accordance with this Use Policy.

Such third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

The Berkeley Police Department is prohibited from selling any ALPR data.

### **1302.10 TRAINING AND ALPR ADMINISTRATOR**

Training for the operation of ALPR ~~Technology~~technology shall be provided by BPD personnel. All BPD employees who utilize ALPR ~~Technology~~technology shall be provided a copy of this Surveillance Use Policy.

(1) The Investigations Division Captain shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(i) Ensuring that training requirements are completed for authorized users. The Administrator shall ensure that members receive department-approved training for those authorized to use or access ALPRs (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

(ii) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52 and this Use Policy

(+)(iii) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### **1302.11 AUDITING AND OVERSIGHT**

Genetec ALPR ~~system~~System audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. ~~(Ref. policy 422.6 (g))~~

1. Any unauthorized access or data breach shall be reported immediately to the City Manager. BPD will enforce against prohibited uses of the Genetec ALPR system, associated ALPR Read and Hit metadata, and lists and databases pursuant to Policy P-26, or other applicable law or policy.
2. The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley website in an appropriate location, and retained within Professional Standards Bureau.

### **1302.12 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under ~~his/her~~their command to administer the day-to-day operation of the ALPR equipment and data. ~~(Ref. policy 422.3)~~

~~1302.12.1~~ ALPR ADMINISTRATOR

~~The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.3.1):~~

- ~~(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.~~
- ~~(b) Training requirements for authorized users.~~
- ~~(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.~~
- ~~(d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.~~
- ~~(e) The title and name of the current designee in overseeing the ALPR operation.~~

~~Ensuring this policy and related procedures are conspicuously posted on the City's website.~~



Surveillance Use Policy- Automated License Plate Reader

Policy  
**1302**

Berkeley Police Department  
Law Enforcement Services Manual

## Surveillance Use Policy- Automated License Plate Reader

### 1302.1 PURPOSE

This Surveillance Use Policy is legally-enforceable pursuant to BMC 2.99.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for Parking Enforcement Operations, Parking Analysis, and limited criminal enforcement purposes associated with Parking Enforcement Operations while recognizing the established privacy rights of the public.

### 1302.2 DEFINITIONS

**"Alleged Parking Violation"** means an alleged violation of time limits in parking areas designated by state and local law, or a violation of time limits and/or non-permit parking in the City's RPP zones.

**"ALPR Read Image"** means images of license plates, vehicles, wheels or any other incidentally captured image.

**"ALPR Read"** means computer-readable data captured by an ALPR Reader, including ALPR Read Image and associated ALPR Read Metadata. ALPR Reads are transient means to create potential government records, to include Parking Analysis data and Enforced Citations.

**"ALPR Hit"** means an Alleged Parking Violation or Stolen Vehicle System alert resulting from computer generated analysis of ALPR Reads by the Genetec ALPR System resulting in an apparent:

1. match between an ALPR Read and ALPR Read Metadata stored in the Genetec ALPR System, to include the Stolen Vehicle System; or
2. cross checking between ALPR Read and permit information which is stored on the Genetec ALPR System.

**"ALPR Read Metadata"** means any image-based or other metadata, including but not limited to, global positioning system coordinates, block face information, tire position information, digitized license plates in alphanumeric characters, and timestamps.

**"Automated License Plate Reader"** or **"ALPR"** means one or more Genetec AutoVu mobile cameras affixed to Parking Enforcement Vehicles and combined with computer software and algorithms to read and convert images of license plates, the characters they contain, and associated ALPR Read Metadata related to Parking Enforcement Operations or Parking Analysis into computer-readable data.

**"Deploy"** or **"Deployment"** means any operation or use of ALPR Readers affixed to Parking

## *Surveillance Use Policy- Automated License Plate Reader*

---

Enforcement Vehicles.

**"Enforced ALPR Hit"** means an Alleged Parking Violation confirmed by a Parking Enforcement Officer that results in the transmission of associated ALPR Read Image and ALPR Read Metadata to the Passport Parking Management System for storage in a database as a government record for the purpose of citation processing.

**"Genetec ALPR System"** means the computerized Genetec server and database that stores all ALPR Reads, metadata and hits, and also pushes an Enforced ALPR Hit metadata to the Passport Parking Management System.

**"Residential Parking Permits"** or **"RPP"** means an annual, visitor, merchant or in-home care parking permit, typically represented by a vehicle's license plate, and associated with the City's Residential Parking Permit program across designated zones.

**"Parking Enforcement Vehicle"** means the GO-4 three-wheeled parking enforcement vehicle.

**"Parking Enforcement Officers"** means employees of the City who work weekly rotations on Parking Enforcement Operations beats throughout the City and are properly trained to operate ALPRs and access the Genetec ALPR System.

**"Parking Enforcement Operations"** means Parking Enforcement Officer enforcement of parking regulations associated with local ordinances, the California Vehicle Code, and Stolen Vehicle System enforcement through Parking Enforcement Vehicle-based automated (ALPR) and non-automated means.

**"Personally Identifiable Information"** or **"PII"** means information:

1. that directly identifies an individual (e.g., name, address, telephone number, email address, etc.) or
2. by which the City or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

**"Parking Analysis"** means ongoing computational or algorithmic analyses performed by the City of Berkeley on ALPR Read Metadata regarding the occupancy of total parking spaces across commercial districts as part of goBerkeley, the City's data-driven, demand-responsive parking management program. ALPR Read Metadata data associated with Parking Analysis may include non-randomized license plates, to be maintained by Public Works for Parking Analysis.

**"Parking Permit Application"** means an application submitted to the City for RPP or other permit that may include but is not limited to PII such as names, address, photo identification, vehicle registration (license plate and vehicle identification number), phone number and email address.

**"Passport Automatic Data Collection System"** means the server and database whereby the Passport Parking Management System vendor, on behalf of the City, downloads, stores and transfers Parking Analysis ALPR Read Metadata stripped of any and all PII before being transferred to the goBerkeley program.

**"Passport Parking Management System"** means the servers and databases maintained by Passport Labs Incorporated, containing the database of the license plate numbers and other PII associated with Parking Permit Applications and Residential Parking Permits, and including historic parking citation data, to include Enforced Hits.

### *Surveillance Use Policy- Automated License Plate Reader*

---

"**OPSMAN Mobile**" means a mobile device providing handheld ticket issuance and ALPR data reference capabilities.

"**Stolen Vehicle System**" or "**SVS**" means information from the California Law Enforcement Telecommunications System's (CLETS) Department of Justice (DOJ) Stolen Vehicle System (SVS) database providing data regarding wanted and stolen vehicles.

#### **1302.3 AUTHORIZED AND PROHIBITED USES**

Use of an ALPR is restricted to the purposes outlined below.

All data and images gathered by the ALPR are for official use by the Berkeley Police Department (BPD) for Parking Enforcement Operations and may be retroactively queried in limited circumstances only as specified by this policy and/or federal, state, local law.

ALPR data may be used by the Finance, Information Technology (IT), Customer Service, and Public Works Departments only as specified in this policy, and consistent with Parking Enforcement Operations and Parking Analysis. Data that is considered confidential pursuant to case law, state statutes, and BPD Policy 804 Records Release Management and/or applicable federal, state, or local law is not open to public review.

Berkeley Police Department members or other Departments shall not use, or allow others to use the equipment or database records for any unauthorized purpose, and will enforce this policy pursuant to Section 1302.11(1).

- (a) An ALPR shall only be Deployed and used for Parking Enforcement Operations, and Parking Analysis.
- (b) ALPR data obtained from Parking Enforcement Operations and retained pursuant to this use policy, including data and metadata associated with ALPR Reads and Hits, may be queried and used to support a specific BPD criminal investigation when an officer has a good faith belief that an emergency involving the danger of, or imminent threat of death or serious physical injury to any person requires such a query or use, and the officer reasonably believes there is a nexus between a vehicle and the alleged crime scene. Approval to query or use the data must be granted by the Chief of Police and City Manager. The City Manager shall log any queries or use of such information pursuant to this subsection in its Annual Surveillance Technology Report pursuant to BMC 2.99.
- (c) Notwithstanding subsection (b), officers may investigate hits based on reasonable suspicion resulting from apparent matches, discovered in the regular course of work of Parking Enforcement Operations, between the Genetec ALPR System and the following databases: Stolen Vehicles System, Amber, Silver, and Blue Alerts, local missing persons, scoff law violator, gig car, general permit, or other non-criminal local lists.
- (d) Data obtained from Parking Analysis shall not be queried or used for criminal investigations.
- (e) The following uses of the Genetec ALPR System are specifically prohibited:
  1. Invasion of Privacy
    - (a) It is a violation of this Policy to utilize the Genetec ALPR System to capture license plates not on a public road or street, or in a place not accessible to the public.

### *Surveillance Use Policy- Automated License Plate Reader*

---

2. Crowd Control
  - (a) ALPRs shall not be deployed in crowd control operations except strictly for the purposes of Parking Enforcement Operations.
3. Criminal Enforcement
  - (a) It is a violation of this Policy to use or Deploy ALPRs to scan or canvass license plates in connection with any crime scene, patrol operation, or investigation except pursuant to Section 1302.3(c) of this Policy.
4. Use of Lists and Databases
  - (a) It is a violation of this Policy to use the Genetec ALPR System or associated ALPR Read data in conjunction with any list or database other than those specified pursuant to Section 1302.3(c) of this Policy, or for any personal use.

#### **1302.4 DATA COLLECTION AND RETENTION**

The Investigations Division Captain, or their designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT) Department and associated Genetec ALPR system providers/vendors as identified below.

IT's role will be limited to providing initial infrastructure set-up and accessing or viewing individual records or reports (potentially including PII or CLETS information as authorized by the Chief of Police), and testing the accuracy of the equipment. Genetec ALPR System data provided to Parking Control Officers may also contain confidential CLETS information and is not open to public review.

##### **(a) ALPR Read Images**

ALPR Reads Images are license plate images which are uploaded daily Genetec server and shall be purged pursuant to the retention guidelines in subsection (b).

##### **(b) ALPR Reads Not Resulting in ALPR Hits**

All ALPR Read Images and ALPR Read Metadata transmitted to and stored in the Genetec ALPR System shall be purged within fourteen (14) days to allow for the City's enforcement of its 72-Hour Rule (BMC Section 14.36.050).

ALPR Read Metadata in the form of license plate data or other non-PII data may be transmitted to and stored in the Passport Automatic Data Collection System for Parking Analysis purposes and retained pursuant to applicable retention policies.

##### **(c) ALPR Hits**

All ALPR Hits and related metadata resulting from ALPR Reads should be uploaded daily to the Genetec server and shall be purged from Genetec within fourteen (14) days to allow for the City's enforcement of its 72-Hour Rule (BMC Section 14.36.050).

##### **(d) Unenforced ALPR Hits**

### *Surveillance Use Policy- Automated License Plate Reader*

---

All erroneous and unenforced ALPR Hit data shall be purged locally at least nightly.

#### (e) Enforced ALPR Hits

Only ALPR Read Images and Metadata associated with Enforced ALPR Hits shall be downloaded to the Passport Parking Management System servers, with a maximum retention period of one (1) year in Passport and in accordance with the established records retention schedule.

### **1302.5 DATA ACCESS**

- (a) Only properly trained Parking Enforcement Officers, Sworn Officers as selected by the Investigation's Division Captain, and Information Technology personnel are allowed access to the Genetec ALPR system or to collect ALPR information.
- (b) No member of the BPD shall operate ALPR equipment or access ALPR data without first completing department-approved training, which shall include compliance with this use policy.
- (c) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (d) If a Sworn officer is called to verify a stolen vehicle, if practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR Hit.
- (e) Sworn Officers shall visually verify that the license plate of interest matches identically with the ALPR Read Image of the license plate number captured (ALPR Read) by the ALPR, including both the alphanumeric characters of the license plate, state of issue, and vehicle descriptors before proceeding. BPD members alerted to the fact that an observed motor vehicle's license plate is entered as an ALPR Hit in a specific Stolen Vehicle System list are required to make a reasonable effort to confirm that a wanted person is actually in the vehicle and/or that a reasonable basis exists before a Department member would have a lawful basis to stop the vehicle.

### **1302.6 DATA PROTECTION**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

- (a) All ALPR data downloaded to any workstation or server shall be accessible only through a login and/or password-protected system capable of documenting all access of information by name, date and time.
- (b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for Parking Enforcement Operations or

## *Surveillance Use Policy- Automated License Plate Reader*

---

specific BPD criminal or civil investigations authorized by a court order, subpoena, or search warrant.

- (c) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question. If a Berkeley Police Department member becomes aware of an inaccurate manual entry into the ALPR databases, that member shall immediately contact the originating agency or officer to notify the agency of the inaccuracy. The member shall then notify both the Investigations Division Captain and the Inspections and Audit Sergeant of the data error for appropriate follow up and tracking.

### **1302.7 CIVIL LIBERTIES AND RIGHTS PROTECTION**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal, state, and local law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third-Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to impacts that may violate the First and Fourth Amendments and other potentially disparate or adverse impacts on any communities or groups.

The Berkeley Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for the purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

### **1302.8 PUBLIC ACCESS**

Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of their identity and of ownership of the vehicle in question. All requests will be evaluated on a case-by-case basis to ensure they conform to the requirements and limitations of public records requests and other applicable law.

### **1302.9 THIRD PARTY DATA-SHARING**

(a) Non-law enforcement requests for anonymized ALPR bulk data related to parking enforcement and access to stored ALPR data related to parking management shall be processed according to this policy, the Records Maintenance and Release Policy and applicable federal, state, and local law.

### *Surveillance Use Policy- Automated License Plate Reader*

---

(b) The ALPR data may be shared only with other law enforcement or prosecutorial agencies as pursuant to a valid court order, subpoena, or a search warrant, Cal. Civ. Code § 1798.90.55(b), and as permitted by this policy and shall not be shared with federal immigration enforcement officials consistent with this policy and other applicable City policy.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided by this policy and the Records Maintenance and Release Policy.

Aggregated ALPR data not related to specific criminal or civil investigations authorized by a court order, subpoena, or search warrant shall not be released to any local, or state agency or entity without the express written consent of the City Manager and only in accordance with this Use Policy.

Such third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

The Berkeley Police Department is prohibited from selling any ALPR data.

#### **1302.10 TRAINING AND ALPR ADMINISTRATOR**

Training for the operation of ALPR technology shall be provided by BPD personnel. All BPD employees who utilize ALPR technology shall be provided a copy of this Surveillance Use Policy.

(1) The Investigations Division Captain shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(i) Ensuring that training requirements are completed for authorized users. The Administrator shall ensure that members receive department-approved training for those authorized to use or access ALPRs (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

(ii) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52 and this Use Policy

(iii) Ensuring this policy and related procedures are conspicuously posted on the City's website.

#### **1302.11 AUDITING AND OVERSIGHT**

Genetec ALPR System audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

1. Any unauthorized access or data breach shall be reported immediately to the City Manager. BPD will enforce against prohibited uses of the Genetec ALPR system, associated ALPR Read and Hit metadata, and lists and databases pursuant to Policy P-26, or other applicable law or policy.
2. The audit shall be documented in the form of an internal department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be placed into the annual report filed with the City Council pursuant to BMC Section 2.99.020 2. d., published on the City of Berkeley

*Surveillance Use Policy- Automated License Plate Reader*

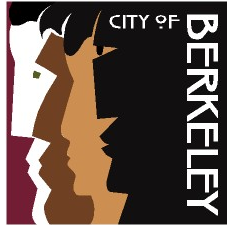
---

website in an appropriate location, and retained within Professional Standards Bureau.

**1302.12 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under their command to administer the day-to-day operation of the ALPR equipment and data.





Kate Harrison  
Councilmember District 4

## **REVISED AGENDA MATERIAL for Supplemental Packet 1**

**Meeting Date:** February 25, 2020

**Item Number:** 23

**Item Description:** Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras

**Submitted by:** Councilmember Harrison

### **Revisions**

Revised the following Berkeley Police Department (BPD) proposed Policies 422, Policy 1302 and 1302(a) as follows:

1. Clarified that the intended purpose of ALPR technology is to capture and store digital license plate data and images for parking and scofflaw enforcement, while also recognizing data retained by BPD (limited to positive ALPR hits) may only be used to support specific criminal investigations.
2. Removed blanket provision that reasonable suspicion or probable cause is not required before ALPR use.
3. Removed ALPR crime scene canvass provision and blanket policy of entering plates into the ALPR system in an attempt to identify suspect vehicles.
4. Clarified that it shall be a violation of City policy to share a login with anyone outside of the City of Berkeley, except in cases of disaster or emergency that do not allow time for proper procedures to be followed.
5. Clarified that unauthorized access or data breaches shall be reported immediately to the City Manager.

6. Consistent with the Surveillance Ordinance BMC 2.99.020 (2) (a), clarified that third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification.

## **Rationale**

Proposed Policies 1302 and 422 inappropriately expand the scope of permitted deployments of Automated License Plate Readers (ALPR) to “support criminal investigations” and “canvass license plates around any crime scene.” Both policies instruct officers that “[p]artial license plates reported during major crimes should be entered into the ALPR system in any attempt to identify suspect vehicles.”<sup>1</sup>

Council has neither given policy nor budgetary approval for such proposed ALPR uses and therefore the Resolution as proposed by staff should not be accepted without revision.

The proposed BPD Policies 1302 and 422 are inconsistent with the scope of the following effective Council and BPD policies regarding ALPR:

1. *Resolution No. 68,085-N.S.*

- Resolution No. 68,085-N.S. authorizes the collection of ALPR data for a single use: anonymized parking data supporting the goBerkeley parking program.

2. July 11, 2017 City Council Annotated Agenda

- The Annotated Agenda notes Council direction to the City Manager to amend Section 7.f of General Administrative Order #0001-2016 to defer any release of data until the surveillance policy and ordinance are adopted. To date, the City Manager has not amended Order #0001-2016.

3. *BPD General Administrative Order #001-2016*

- Section 1 of the effective BPD General Administrative Order #001-2016 specifies that only the BPD Parking Enforcement and Traffic Units may use ALPRs.
- Section 9 specifies further that “parking and scofflaw enforcement” are the only permitted use and deployment for ALPR technology in the City of Berkeley.

4. *Contract No. 9977*

- The scope of Contract No. 9977 is limited to the purchase of ALPR units in service of parking enforcement activities.

## **Attachments**

---

<sup>1</sup> Sections 1302.2 (b) - (c); Sections 422.4 (b) - (c).

1. Revised Policies 422, Policy 1302 and 1302(a)
2. July 11, 2017 City Council Annotated Agenda
3. BPD General Administrative Order #001-2016
4. Contract No. 9977

PROPOSED D4 AMENDMENTS

**BPD Policy Manual 422**

**Automated License Plate Readers (ALPRs)**

**422.1 PURPOSE AND SCOPE**

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

**422.2 POLICY**

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for parking and scofflaw enforcement while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

**422.3 ADMINISTRATION**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

**422.3.1 ALPR ADMINISTRATOR**

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

**422.4 USE OF THE ALPR**

The intended purpose of an ALPR shall only be used is for official law enforcement business parking and scofflaw enforcement.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

PROPOSED D4 AMENDMENTS

(a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.

(b) ~~An ALPR data obtained from parking and scofflaw enforcement may be used to support a specific criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.~~

~~(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.~~

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System

(CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

**422.5 DATA COLLECTION AND RETENTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review.

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance shall be provided by the City of Berkeley's Information

Technology (IT Department and associated ALPR system providers/vendors as identified below.

IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

(a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.

(b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not showing violations will not be transferred to the server.

**422.6 ACCOUNTABILITY**

PROPOSED D4 AMENDMENTS

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code§ 1798.90.51; Civil Code§ 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code§ 1798.90.52). It shall be a violation of this policy to share a login with anyone outside of the City of Berkeley, except in cases of disaster or emergency that do not allow time for proper procedures to be followed.
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. For security or data breaches, see the Records Release and Maintenance Policy. Any unauthorized access or data breach shall be reported immediately to the City Manager.

**422.7 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  - 1. The name of the agency.
  - 2. The name of the person requesting.
  - 3. The intended purpose of obtaining the information.
  - 4. The related case number.

PROPOSED D4 AMENDMENTS

(b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.

(c) The approved request is retained on file. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

Third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 (2) (a).

**422.8 SCOFFLAW ENFORCEMENT**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "go Berkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit

**PROPOSED D4 AMENDMENTS**

violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.



PROPOSED D4 AMENDMENTS

**Surveillance Use Policy - ALPR**

**1302.1 PURPOSE**

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by BMC 2.99.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images for parking and scofflaw enforcement while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. (Ref. policy 422.2)

**1302.2 AUTHORIZED AND PROHIBITED USES USE**

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53). (Ref. policy 422.4)

(a) ~~The intended purpose of An ALPR shall only be used is~~ for parking and scofflaw enforcement. ~~official law enforcement business.~~

(b) ~~An ALPR data obtained from parking and scofflaw enforcement~~ may be used to support a ~~patrol operation or specific~~ criminal investigation. ~~Reasonable suspicion or probable cause is not required before using an ALPR.~~

~~(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.~~

**1302.3 DATA COLLECTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law. (Ref. policy 422.5)

**1302.4 DATA ACCESS**

(a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

PROPOSED D4 AMENDMENTS

(c) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

**1302.5 DATA PROTECTION**

All saved data will be safeguarded and protected by both procedural and technological means.

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code§ 1798.90.51; Civil Code§ 1798.90.53) (Ref. policy 422.6):

(a) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52). It shall be a violation of this policy to share a login with anyone outside of the City of Berkeley, except in cases of disaster or emergency that do not allow time for proper procedures to be followed.

(b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.

(c) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

(d) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question. Any unauthorized access or data breach shall be reported immediately to the City Manager.

**1302.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

**1302.7 DATA RETENTION**

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the

City of Berkeley's Information Technology (IT) department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role

## PROPOSED D4 AMENDMENTS

will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)

(a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

### 1302.8 PUBLIC ACCESS

(a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. (Ref. policy 422.6 (a))

(b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requester in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question. (Ref. policy 422.6 (b))

### 1302.9 THIRD-PARTY DATA-SHARING

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. ALPR data is subject to the provisions of BPD Policy 415, and hence may not be shared with federal immigration enforcement officials.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

[Third-party data-sharing shall be subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 \(2\) \(a\).](#)

(Ref. policy 422.6 (e))

### 1302.10 TRAINING

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

### 1302.11 AUDITING AND OVERSIGHT

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. (Ref. policy 422.6 (g))

### 1302.12 MAINTENANCE

PROPOSED D4 AMENDMENTS

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division

Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. (Ref. policy 422.3)

1302.12.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq.

This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.3.1):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

PROPOSED D4 AMENDMENTS

1302 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT-AUTOMATED LICENSE PLATE READER DEVICES

AUTOMATED LICENSE PLATE READER (ALPR) DEVICES

Automated License Plate Readers (ALPRs) are high-speed, computer controlled camera systems that are typically mounted on Berkeley Police Department Parking Enforcement

**Vehicles.**

ALPRs capture license plate numbers which come into view, along with the location, date and time. The data, which includes a photo of the front or the back of the car displaying the license plate, is then uploaded to a central server.

**B. PURPOSE**

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the California Law Enforcement Telecommunications System's (CLETS) Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

**C. LOCATION**

Parking Enforcement vehicles travel throughout the city; using the ALPRs as described above.

**D. IMPACT**

The Berkeley Police Department is dedicated to promoting public safety with the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with ALPR Units will help to ensure unauthorized use of its data. The procedures will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

**E. MITIGATION**

All saved data will be safeguarded and protected by both procedural and technological means which are implemented to safeguard the public from any impacts identified in subsection (D).

PROPOSED D4 AMENDMENTS

See subsection (G) for further.

**F. DATA TYPES AND SOURCES**

Photographs of license plates and location data may be obtained through the use of ALPR Units.

**G. DATA SECURITY**

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code§ 1798.90.51; Civil Code§ 1798.90.53):

1. All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code§ 1798.90.52). It shall be a violation of this policy to share a login with anyone outside of the Berkeley Police Department, except in case of disaster or emergency that does not allow time for proper procedures to be followed.
2. Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department related civil or administrative action and parking enforcement.
3. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
4. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

**H. FISCAL COST**

In 2015, Public Works brought an ALPR Contract to City Council. Council approved a contract for Public Works to buy five Genetec ALPR Units with PCS Mobile communication, for a pilot program for \$450,000.

In 2017, after success with the program, City Council approved an amendment to the contract, allowing Public Works to purchase 15 more ALPR Units for Parking Enforcement vehicles, and to continue its use of PCS Mobile, for 1,200,000. The money was allocated from the goBerkeley/Federal Highway Administration Parking Meter Fund.

Yearly service for the ALPR Units includes warranties, hosting services, cellular connection, mobile computing, and training which varies. The costs through fiscal year 2022 are currently estimated at \$1,175,000.

Personnel costs are minimal in that the ALPR Units are used as a resource during normal working hours.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

1. Vendor Access-Scofflaw Enforcement: The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

**PROPOSED D4 AMENDMENTS**

a. All data captured by the ALPR is stored on the booting vehicle's laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

b. When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

2. Vendor Access-General Parking Enforcement and goBerkeley Program: The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.

a. In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle.

Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.

b. The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

3. Department of Information Technology Access: Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

4. Other Law Enforcement Agency Access: ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Requests for ALPR data by non-law enforcement or nonprosecutorial agencies will be processed as provided in the Records Maintenance and

Release Policy (Civil Code§ 1798.90.55). Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.

5. Member Access: No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training. No ALPR operator may access CLETS data unless

PROPOSED D4 AMENDMENTS

otherwise authorized to do so. If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.

6. Public Access: Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

[7. Third-party data-sharing is subject to non-privileged and non-confidential City Council notification pursuant to BMC 2.99.020 \(2\) \(a\).](#)

**J. ALTERNATIVES**

None.

**K. EXPERIENCE OF OTHER ENTITIES**

The use of ALPR technology is common amongst law enforcement agencies throughout the country, in support of parking enforcement, and law enforcement criminal investigations.



**ANNOTATED AGENDA  
BERKELEY CITY COUNCIL MEETING**

**Tuesday, July 11, 2017**

**6:00 P.M.**

COUNCIL CHAMBERS - 2134 MARTIN LUTHER KING JR. WAY

JESSE ARREGUIN, MAYOR

Councilmembers:

DISTRICT 1 – LINDA MAIO  
DISTRICT 2 – CHERYL DAVILA  
DISTRICT 3 – BEN BARTLETT  
DISTRICT 4 – KATE HARRISON

DISTRICT 5 – SOPHIE HAHN  
DISTRICT 6 – SUSAN WENGRAF  
DISTRICT 7 – KRISS WORTHINGTON  
DISTRICT 8 – LORI DROSTE

**Preliminary Matters**

**Roll Call:** 6:03 p.m.

**Present:** Bartlett, Davila, Droste, Hahn, Maio, Wengraf, Worthington, Arreguin

**Absent:** Harrison

Councilmember Harrison present 6:14 p.m.

**Ceremonial Matters:**

1. Recognition of UN Association of California, Alpha Kappa Alpha, and Alpha Nu Omega

**City Auditor Comments:**

1. Recognition of Public Works for completing the Equipment Fund Audit

**City Manager Comments:**

1. Launch of Berkeley Bike Share Program on July 11, 2017

**Public Comment on Non-Agenda Matters:** 3 speakers.

**Public Comment on Consent Calendar and Information Items Only:** 1 speakers.

**Consent Calendar**

**Action:** M/S/C (Maio/Worthington) to adopt the Consent Calendar in one motion except as indicated.

**Vote:** All Ayes.

## Consent Calendar

- 1. Referral Response: Healthy Default Beverages with Children’s Meals; Adding BMC Chapter 12.72**  
**From: City Manager**  
**Recommendation:** Adopt second reading of Ordinance No. 7,560-N.S. adding Berkeley Municipal Code (BMC) Chapter 12.72 to require that any food vendor that sells a children’s meal with a beverage included shall make the default beverage offered with the children’s meal either water or milk, with no added sweeteners.  
**First Reading Vote:** All Ayes.  
**Financial Implications:** See report  
Contact: Paul Buddenhagen, Housing and Community Services, 981-5400  
**Action:** Adopted second reading of Ordinance No. 7,560-N.S.
- 2. Technical Corrections to the Zoning Ordinance, Amending Berkeley Municipal Code Sub-Titles 23D and 23E**  
**From: City Manager**  
**Recommendation:** Adopt second reading of Ordinance No. 7,561-N.S. amending Berkeley Municipal Code Sub-Titles 23D and 23E to make non-substantive, technical corrections to the Zoning Ordinance.  
**First Reading Vote:** All Ayes.  
**Financial Implications:** None  
Contact: Timothy Burroughs, Planning and Development, 981-7400  
**Action:** Adopted second reading of Ordinance No. 7,561-N.S.
- 3. Changes to Affordable Housing Mitigation Fee; Amending Berkeley Municipal Code Section 22.20.065**  
**From: City Manager**  
**Recommendation:** Adopt second reading of Ordinance No. 7,562-N.S. amending BMC Section 22.20.065 related to the Affordable Housing Mitigation Fee.  
**First Reading Vote:** Ayes – Maio, Davila, Bartlett, Harrison, Hahn, Wengraf, Worthington, Arreguin; Noes – None; Abstain - Droste; Absent – None  
**Financial Implications:** See report  
Contact: Zach Cowan, City Attorney, 981-6950  
**Action:** Adopted second reading of Ordinance No. 7,562-N.S.
- 4. FY 2018 Annual Appropriations Ordinance**  
**From: City Manager**  
**Recommendation:** Adopt second reading of Ordinance No. 7,563-N.S. adopting the FY 2018 Annual Appropriations Ordinance (AAO) in the amount of \$476,396,570 (gross appropriations) and \$424,590,046 (net appropriations).  
**First Reading Vote:** All Ayes.  
**Financial Implications:** See report  
Contact: Teresa Berkeley-Simmons, Budget Manager, 981-7000  
**Action:** Adopted second reading of Ordinance No. 7,563-N.S.

## Consent Calendar

- 5. Housing Trust Fund Recommendation – Harper Crossing**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution: 1) Approving a Housing Trust Fund (HTF) reservation for Satellite Affordable Housing Associates' Harper Crossing in the amount of \$285,464, and 2) Authorizing the City Manager to execute all original or amended documents or agreements to effectuate this action.  
**Financial Implications:** See report  
 Contact: Paul Buddenhagen, Housing and Community Services, 981-5400  
**Action:** Adopted Resolution No. 68,077–N.S.
- 6. Housing Trust Fund Recommendation – Northern California Land Trust (NCLT) Scattered Site Rehabilitation**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution reserving funds for Northern California Land Trust's Scattered Sites rehabilitation, specifically by: 1. Waiving Section III.A.1 of the Housing Trust Fund (HTF) Guidelines and accepting NCLT as an eligible developer despite its lack of recent experience. 2. Adopting a finding that a City subsidy in excess of 40% of total development costs is justified by the nature of Northern California Land Trust's Scattered Site Rehab and unavailability of alternative funding, as required by the HTF Guidelines, Section V.B.7. 3. Approving a HTF reservation for Northern California Land Trust's Scattered Site Rehab project, in the amount of \$569,692. 4. Authorizing City Manager to refinance the Scattered Site Rehab properties' outstanding HTF loans, with a combined balance currently estimated at \$695,000, into the new development loan with terms consistent with the HTF Guidelines. 5. Authorizing the City Manager to execute all original or amended documents or agreements to effectuate these actions. 6. Recommending that Council recommend to the Northern California Land Trust that the organization move towards establishing a Board of Directors' structure consistent with current community land trust model standards.  
**Financial Implications:** See report  
 Contact: Paul Buddenhagen, Housing and Community Services, 981-5400  
**Action:** Moved to Action Calendar. 4 speakers. M/S/C (Maio/Harrison) to adopt Resolution No. 68,078–N.S. revised to add the two Whereas clauses below, and to direct staff to include the conversion language in the loan documents with NCLT.

*BE IT FURTHER RESOLVED that NCLT educate all current tenants about the benefits of transitioning to a limited equity co-op structure, subsequently begin negotiations to make the conversion to a limited equity co-op structure, and collaborate with an organization that has the capacity and experience to conduct the education and advise on the conversion process.*

*BE IT FURTHER RESOLVED that NCLT submit quarterly financial reports and annual reports relaying the status of their financial situation and progress in changing the structure of the Board of Directors and transition to a limited equity co-op.*

**Vote:** All Ayes.

## Consent Calendar

- 7. Classification and Salary: Homeless Services Coordinator**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution amending Resolution No. 67,484-N.S. Classification and Salary Resolution for Public Employees Union - Local One, to establish the classification of Homeless Services Coordinator with a monthly salary range of \$8,200 - \$9,915 effective July 11, 2017.  
**Financial Implications:** See report  
Contact: Sarah Reynoso, Human Resources, 981-6800  
**Action:** Adopted Resolution No. 68,079–N.S.
- 8. Contract: AMS.NET for Network Equipment and Maintenance**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute a contract with AMS.NET, Inc. for network hardware, support, and maintenance, for a total not to exceed \$455,335 from July 1, 2017 to June 30, 2020.  
**Financial Implications:** Capital Improvement Fund - \$455,335  
Contact: Savita Chaudhary, Information Technology, 981-6500  
**Action:** Adopted Resolution No. 68,080–N.S.
- 9. Contract No. 10522 Amendment: Redwood Engineering Construction for Willard Park Play Area and Pathway Renovations Project**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to amend Contract No. 10522 with Redwood Engineering Construction for the Willard Park Play Area and Pathway Renovation project, increasing the amount by \$115,000 for an amended total amount not to exceed \$417,400.  
**Financial Implications:** Parks Tax Fund - \$417,400  
Contact: Scott Ferris, Parks, Recreation and Waterfront, 981-6700  
**Action:** Adopted Resolution No. 68,081–N.S.
- 10. Contract No. 9044 Amendment: Building Opportunities for Self Sufficiency (BOSS)**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute an amendment to Contract No. 9044 with Building Opportunities for Self Sufficiency for leaf and litter abatement services increasing the contract amount by \$120,000 for a total not to exceed \$1,722,500.  
**Financial Implications:** Zero Waste Fund - \$120,000  
Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,082–N.S.

## Consent Calendar

- 11. Contract No. 9488B Amendment: Berry Brothers Towing for Towing Services**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute an amendment to Contract No. 9488B with Berry Brothers Towing to provide towing services for Department of Public Works Equipment Maintenance, increasing the contract amount \$20,000 for an amended total not to exceed of \$110,000.  
**Financial Implications:** Equipment Maintenance Fund - \$20,000  
 Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,083–N.S.
- 12. Contract No. 9730A Amendment: Fairbanks Scales, Inc.**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute an amendment to Contract No. 9730A with Fairbanks Scales, Inc. for preventative maintenance and repairs on various scales at the City’s Solid Waste Management and Transfer Station, increasing the contract amount by \$50,000 for a total contract amount not to exceed \$140,000, and extending the term of the contract to June 30, 2019.  
**Financial Implications:** Zero Waste Fund - \$50,000  
 Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,084–N.S.
- 13. Contract No. 9977 Amendment: Portable Computer Systems dba PCS Mobile to Purchase 15 Automated License Plate Recognition (ALPR) Units**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute an amendment to Contract No. 9977 with Portable Computer Systems dba PCS Mobile to purchase fifteen additional Automated License Plate Recognition units to increase parking enforcement operations capacity and effectiveness, and increasing the total \$1,200,000 for a new amount not to exceed \$1,650,000, and extending the term from May 30, 2020 to June 30, 2022.  
**Financial Implications:** Parking Meter Fund - \$1,200,000  
 Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Moved to Action Calendar. 8 speakers. M/S/C (Worthington/Wengraf) to adopt Resolution No. 68,085–N.S. authorizing the City Manager to execute an amendment to Contract No. 9977 with Portable Computer Systems dba PCS Mobile to purchase fifteen additional Automated License Plate Recognition units to increase parking enforcement operations capacity and effectiveness, and increasing the total \$1,200,000 for a new amount not to exceed \$1,650,000, and extending the term from May 30, 2020 to June 30, 2022; and amend Section 7.f of Administrative Order #0001-2016 to defer any release of data until the surveillance policy and ordinance are adopted.  
**Vote:** Ayes – Maio, Harrison, Wengraf, Worthington, Droste, Arreguin; Noes – Davila, Bartlett, Hahn.

## Consent Calendar

- 14. Contract No. 10472 Amendments: ELS Architecture & Urban Design and Contract No. 10464 Noll & Tam Architects: On-Call Architectural Services**  
**From: City Manager**  
**Recommendation:** Adopt two Resolutions authorizing the City Manager to execute amendments to the following contracts for on-call architectural services for a combined total of \$2,000,000 as follows:  
1. ELS Architecture and Urban Design, Contract No. 10472, increasing the contract amount by \$1,000,000, for a total not-to-exceed amount of \$1,500,000 and extending the contract period through June 30, 2019;  
2. Noll & Tam Architects, Contract No. 10464, increasing the contract amount by \$1,000,000, for a total not-to-exceed amount of \$1,500,000 and extending the contract period through June 30, 2019.  
**Financial Implications:** Various Funds - \$2,000,000  
Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,086–N.S. (ELS) and Resolution No. 68,087–N.S. (Noll & Tam)
- 15. Contract: Chrisp Company for Roadway Thermoplastic Markings**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution approving plans and specifications for the Roadway Thermoplastic Markings Project, 16-11078-C; and authorizing the City Manager to execute a five year contract period from July 1, 2017 through June 30, 2022, and any amendments, extensions or other change orders until completion of the project in accordance with the approved plans and specifications with Chrisp Company in an amount not to exceed \$1,250,000.  
**Financial Implications:** Various Funds - \$1,250,000  
Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,088–N.S.
- 16. Contract: Clean Harbors, Inc. for Hazardous Waste Management Services**  
**From: City Manager**  
**Recommendation:** Adopt a Resolution authorizing the City Manager to execute a contract with Clean Harbors, Inc. for hazardous waste management, removal, and disposal services for the City of Berkeley in an amount not-to-exceed \$150,000 for the period August 1, 2017 through June 30, 2020.  
**Financial Implications:** Various Funds - \$150,000  
Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Adopted Resolution No. 68,089–N.S.

## Consent Calendar

17. **Mitigating Impacts of Outdoor Air Quality on Indoor Air Quality in Berkeley**  
**From: Community Environmental Advisory Commission**  
**Recommendation:** Direct the City Manager to request the Planning Commission use the analyses presented here, and the draft provided in Appendix II, to create new Standard Conditions of Approval (SCA) for new building construction near major sources of air pollution, to achieve an acceptable level of indoor air quality (IAQ) for sensitive receptors. Total spending for required IAQ mitigations shall be at 1-2% of estimated total project costs.  
**Financial Implications:** See report  
Contact: Nabil Al-Hadithy, Commission Secretary, 981-7400  
**Action:** Approved recommendation as modified below.

*Refer the item to the Planning Commission to consider the analyses presented here, and the draft provided in Appendix II, to create new Standard Conditions of Approval (SCA) for new building construction near major sources of air pollution, to achieve an acceptable level of indoor air quality (IAQ) for sensitive receptors.*

18. **Ending Tax Breaks for Private Prisons Act**  
**From: Peace and Justice Commission**  
**Recommendation:** Adopt a Resolution: 1. Directing the City Clerk to send a letter to Rep. Devin Nunes (R-CA) of the Joint Committee on Taxation with copies to all members of the Congressional Joint Committee on Taxation, and the Senate Finance Committee calling on Congress to pass the “Ending Tax Breaks for Private Prisons Act;” and 2. Having the Council of the City of Berkeley sign the MoveOn.org online petition telling congress to end private prison tax breaks.  
**Financial Implications:** None  
Contact: Eric Brenman, Commission Secretary, 981-5400  
**Action:** Moved to Action Calendar. 1 speaker. M/S/C (Worthington/Maio) to adopt Resolution No. 68,090–N.S.

**Vote (Recommendation #1):** All Ayes.

**Vote (Recommendation #2):** Ayes – Maio, Davila, Bartlett, Harrison, Wengraf, Worthington, Droste, Arreguin; Noes – None; Abstain – Hahn.

## Council Consent Items

19. **Vitality of University Avenue**  
**From: Councilmembers Maio, Davila, and Harrison**  
**Recommendation:** Refer to the City Manager and Economic Development to analyze storefront vacancies on University Avenue and make recommendations on how to create a more vibrant streetscape on our main boulevard.  
**Financial Implications:** Staff time  
Contact: Linda Maio, Councilmember, District 1, 981-7110  
**Action:** Approved recommendation.
20. **Support Oakland Public Defender Rodney Brooks' Efforts to Keep In-Custody Arraignment Hearings in Oakland and Not Move Them to the East County Hall of Justice in Dublin**  
**From: Councilmembers Davila and Harrison, and Mayor Arreguin**  
**Recommendation:** Send a letter from Berkeley City Council supporting Oakland Public Defender Rodney Brooks' efforts to keep in-custody arraignment hearings in Oakland and not move them to the East County Hall of Justice in Dublin.  
**Financial Implications:** None  
Contact: Cheryl Davila, Councilmember, District 2, 981-7120  
**Action:** Approved recommendation.
21. **Referral to the Community Environmental Advisory Commission: Cigarette Butt Pollution Prevention Program in South Berkeley** (*Item contains revised materials.*)  
**From: Councilmembers Bartlett and Harrison**  
**Recommendation:** Refer to the Community Environmental Commission (CEAC) to consider developing a Cigarette Butt Pollution Prevention Program for South Berkeley. Explore the following items: a) Location. Work with the local business associations, business owners, as well as other neighborhood and community organizations to identify key locations for cigarette butt receptacles. b) Operation. Work with local businesses to develop a system for cleanup and disposal of the contents of the receptacles. c) Cost. Identify any one-time costs associated with the program, including purchasing and installation of the receptacles. Identify any costs that should be set aside for maintenance. There should not be regular ongoing costs. CEAC should work with the businesses and neighborhoods to develop a community-based system to facilitate daily operations.  
**Financial Implications:** Staff time  
Contact: Ben Bartlett, Councilmember, District 3, 981-7130  
**Action:** Approved recommendation as revised in Supplemental Reports Packet #1 to add Councilmember Harrison as a co-sponsor and add that the item is also referred to the City Manager.



## Council Consent Items

22. **Support for AB 932 – Bill Giving San Francisco and San Diego Flexibility to Build Shelters and Transitional Housing for Unsheltered Homeless Residents From: Councilmembers Bartlett, Hahn, and Davila**  
**Recommendation:** Recommend that the Berkeley City Council send a letter to Senator Nancy Skinner and Governor Jerry Brown urging them to support AB 932.  
**Financial Implications:** None  
Contact: Ben Bartlett, Councilmember, District 3, 981-7130  
**Action:** Approved recommendation with the letter revised to add the following phrase to the last sentence, “and request the addition of the City of Berkeley to the cities included in the bill.”
23. **Support for SB 33: Bill Prohibiting Financial Institutions from Forcing Consumers to Give up Legal Rights when the Bank has Committed Intentional Fraud Against Them**  
**From: Councilmembers Bartlett, Hahn, and Davila**  
**Recommendation:** Recommend that the Berkeley City Council send a letter to Assemblymember Tony Thurmond, and Governor Jerry Brown urging them to support SB 33.  
**Financial Implications:** None  
Contact: Ben Bartlett, Councilmember, District 3, 981-7130  
**Action:** Approved recommendation.
24. **Support of AB 214: Postsecondary Education, Student Hunger** *(Item contains revised materials.)*  
**From: Councilmembers Harrison, Hahn, Davila, and Bartlett**  
**Recommendation:** Adopt a Resolution supporting AB 214 Postsecondary Education, Student Hunger, an act to reduce hunger and homelessness in college students in California, and sending a copy of the resolution to Governor Jerry Brown, and Assemblymembers Lorena Gonzalez Fletcher (Appropriations Chair), Frank Bigelow (Vice Chair), Richard Bloom, Raul Bocanegra, Rob Bonta, William Brough, Ian Calderon, Ed Chau, Susan Talamantes Eggman, Vince Fong, Laura Friedman, James Gallagher, Eduardo Garcia, and Adam Gray.  
**Financial Implications:** Minimal  
Contact: Kate Harrison, Councilmember, District 4, 981-7140  
**Action:** Adopted Resolution No. 68,091–N.S.

## Council Consent Items

25. **Adopt a Resolution Approving the Allocation of \$3,131,651 in Predevelopment from the Housing Trust Fund for the Berkeley Way Project**  
**From: Councilmembers Worthington, Harrison, Hahn, and Mayor Arreguin**  
**Recommendation:** That the Council adopts a Resolution to approve the allocation of \$3,131,651 in Housing Trust Funds for the predevelopment of BRIDGE Housing Corporation and Berkeley Food and Housing Project's Berkeley Way project, in compliance with the Housing Advisory Commission's recommendation, scheduled to be voted on July 6, 2017.  
**Financial Implications:** See report  
Contact: Kriss Worthington, Councilmember, District 7, 981-7170  
**Action:** Adopted Resolution No. 68,092–N.S. as revised in Supplemental Reports Packet #2.
26. **Support California AB 395 to Protect Internet Privacy**  
**From: Councilmember Worthington**  
**Recommendation:** That the Council support California Assembly Bill 395 (AB 395) in its aim to protect the internet security and privacy of Californians.  
**Financial Implications:** See report  
Contact: Kriss Worthington, Councilmember, District 7, 981-7170  
**Action:** Approved recommendation as Revised in Supplemental Reports Packet #2 to correct the bill number to AB 375.

## Action Calendar – Public Hearings

27. **Amending the Berkeley Election Reform Act to Implement Public Financing**  
**From: Fair Campaign Practices Commission**  
**Recommendation:** Conduct a public hearing and upon conclusion, adopt first reading of an Ordinance amending Berkeley Municipal Code 2.12 to make changes to facilitate the implementation of the Berkeley Fair Elections Act of 2016 by a vote of not less than two-third of the City Council, in accordance with procedure for amending the Berkeley Election Reform Act set forth in Berkeley Municipal Code 2.12.051.A.  
**Financial Implications:** See report  
Contact: Jessica Mar, Commission Secretary, 981-6950
- Public Testimony:** The Mayor opened the public hearing. 3 speakers. M/S/C (Worthington/Hahn) to close the public hearing.  
**Vote:** All Ayes.
- Action:** Adopted first reading of Ordinance No. 7,564–N.S. Second reading scheduled for July 25, 2017.  
**Vote:** All Ayes.

## Action Calendar – Old Business

**28a. Automatic Door Openers in Multi-Unit Residential Buildings** *(Continued from May 30, 2017)*

**From: Commission on Disability**

**Recommendation:** Adopt a Resolution requiring: all new construction of multi-unit residential buildings (four or more units) with a common entryway in the City of Berkeley to include automatic door openers; significant remodeling or conversion of residential multi-unit buildings with four or more units and a common entryway to include automatic door openers; and owners of existing multi-unit residential buildings (four or more units) with a common entryway must install automatic door openers at the request of a resident.

**Financial Implications:** Unknown

Contact: Ella Callow, Commission Secretary, 981-6300

**28b. Companion Report: Automatic Door Openers in Multi-Unit Residential Buildings** *(Continued from May 30, 2017)*

**From: City Manager**

**Recommendation:** The City Manager recommends the City Council evaluate the resolution requested by the Commission on Disability as an amendment to BMC § 19.28.010. If Council agrees with the substantive recommendations in the Commission on Disability (CoD) report entitled “Recommendations to Require Inclusion of Automatic Door Openers in Residential Buildings with Four or More Units and a Common Entryway,” the City Manager recommends Council consider a stand-alone ordinance (similar to BMC § 19.80) that would (1) limit the scope to privately owned buildings with four or more units and a common entryway; (2) not subsidize installation of automatic door openers by building owners/builders; (3) include language that limits the City’s responsibility to conduct inspections to ensure compliance; and (4) limit the City’s liability for torts related to automatic door openers that are installed.

**Financial Implications:** See report

Contact: Phillip Harrington, Public Works, 981-6300

**Action:** 2 speakers. M/S/C (Worthington/Maio) to hold over the item to September 12, 2017.

**Vote:** All Ayes.

## Action Calendar – Old Business

29. **Housing Accountability Act** *(Continued from June 13, 2017. Item includes supplemental materials.)*

**From: City Manager**

Contact: Zach Cowan, City Attorney, 981-6950

**Action:** 5 speakers. M/S/C (Arreguin/Davila) to refer to the City Manager, Planning Commission, Zoning Adjustments Board, and Design Review Committee to consider the following actions, and others they may find appropriate, to address the potential impacts of the Housing Accountability Act and to preserve local land use discretion:

1. Amend the General Plan and Zoning Ordinance to adopt numerical density and/or building intensity standards that can be applied on a parcel-by-parcel basis in an easy and predictable manner. These would constitute reliable and understandable “objective general plan and zoning standards” that would establish known maximum densities. This could be done across the board or for specified districts.
2. Devise and adopt “objective, identified written public health or safety standards” applicable to new housing development projects.
3. Adopt “design review standards that are part of ‘applicable, objective general plan and zoning standards and criteria’”.
4. Quantify and set objective zooming standards and criteria under the first sentence of Government Code Section 65589.5(j) for views, shadows, and other impacts that often underlie detriment findings.

**Vote (Paragraphs 1-3):** Ayes – Maio, Davila, Harrison, Hahn, Wengraf, Worthington, Arreguin; Noes – Bartlett, Droste.

**Vote (Paragraph 4):** Ayes – Maio, Davila, Harrison, Hahn, Wengraf, Arreguin; Noes – Bartlett, Droste, Worthington.

Recess: 9:10 p.m. – 9:27 p.m.

30. **Amend BMC Sections 3.78.030, 040, and 050 Related to Commission Procedures** *(Continued from June 13, 2017)*

**From: Human Welfare and Community Action Commission**

**Recommendation:** Adopt a Resolution requesting that the City Manager examine the addition of language to the Berkeley Municipal Code that clarifies aspects of the management of City of Berkeley commissions and the removal and appointment of commissioners.

**Financial Implications:** See report

Contact: Wing Wong, Commission Secretary, 981-5400

**Action:** Moved to Consent Calendar. No action taken by the City Council on this item.

**Vote:** Ayes – Maio, Bartlett, Harrison, Hahn, Wengraf, Worthington, Droste, Arreguin; Noes – Davila.

## Action Calendar – Old Business

- 31. Ordinance to Ban the Sale of Fur in Berkeley; Adding BMC Chapter 9.22**  
**From: Councilmember Worthington** (*Continued from June 13, 2017*)  
**Recommendation:** Adopt second reading of Ordinance No. 7,539-N.S. adding BMC Chapter 9.22 to eliminate the sale of fur apparel products in order to promote community awareness of animal welfare.  
 First Reading Vote: Ayes - Maio, Davila, Bartlett, Hahn, Wengraf, Arreguin; Noes – Harrison, Worthington, Droste; Abstain – None; Absent – None.  
**Financial Implications:** None  
 Contact: Kriss Worthington, Councilmember, District 7, 981-7170  
**Action:** Item held over to July 25, 2017.
- 32. Support the Resilient Shoreline Program of Citizens for East Shore Parks**  
*(Continued from June 27, 2017)*  
**From: Mayor Arreguin and Councilmembers Hahn, Wengraf, and Maio**  
**Recommendation:** Adopt a Resolution supporting the Resilient Shoreline Program of Citizens for East Shore Parks (CESP) to raise awareness about the detrimental effects of sea-level rise and promote resilient shoreline solutions. Additionally, refer to the mid-year budget process a contribution of \$10,000 to participate in CESP’s Visualizing Sea-level Rise event in Berkeley.  
**Financial Implications:** General Fund - \$10,000  
 Contact: Jesse Arreguin, Mayor, 981-7100  
**Action:** Moved to Consent Calendar. Adopted Resolution No. 68.093–N.S. in support of the Resilient Shoreline Program, and Resolution No. 68,094–N.S. to authorize the expenditure of surplus funds from the Mayor’s and Councilmembers’ expense accounts for CESP from the following Councilmembers up to amounts listed: Mayor Arreguin - \$2,000; Councilmember Wengraf - \$500; Councilmember Maio - \$250; Councilmember Harrison - \$250; Councilmember Davila - \$250.
- 33. Expedited Review for Affordable Housing Projects** (*Continued from June 27, 2017. Item contains revised materials.*)  
**From: Councilmembers Hahn, Davila, and Bartlett**  
**Recommendation:** 1. Refer to the City Manager the creation of an expedited review process for housing projects in which Affordable Housing units make up more than 20% of the proposed on-site units; and  
 2. Direct the City Manager to immediately confer priority status and offer expedited review to 100% Affordable projects, pending adoption of a more formal and widely applicable expedited review process.  
**Financial Implications:** Staff time  
 Contact: Sophie Hahn, Councilmember, District 5, 981-7150  
**Action:** Item held over to July 25, 2017.

## Action Calendar – Old Business

34. **General Fund Stability Reserve Usage Criteria** *(Continued from June 27, 2017. Item contains revised materials.)*

**From: Councilmembers Droste, Wengraf, and Maio**

**Recommendation:** Discuss the General Fund Stability Reserve Usage Policies described in the report and adopt policies such as those proposed, requiring a two-thirds vote of the City Council to amend them. Following recommendation from the City Manager, the City Council shall, from time to time, recognize and define “essential services”, “appropriate levels” of such services, and “extreme conditions”. Any draw-down of Stability Reserve funds shall coincide with the adoption of a plan to repay the dollar amount of the draw down. If adopting a repayment plan immediately is infeasible due to emergency circumstances, it shall be adopted no more than 3 months from the date of the withdrawal appropriation. The level of the Stability Reserve shall be restored as economic recovery occurs, consistent with the maintenance of essential services, with repayment to begin no more than 5 years from the date of withdrawal and be completed within 10 years from the date of withdrawal.

**Financial Implications:** See report

Contact: Lori Droste, Councilmember, District 8, 981-7180

**Action:** 4 speakers. M/S/C (Hahn/Arreguin) to continue the item to September 26, 2017.

**Vote:** All Ayes.

## Action Calendar – Old Business

### 35. **Medical Cannabis Cultivation Ordinance Revisions** *(Continued from June 27, 2017. Item contains revised materials.)*

**From: City Manager**

**Recommendation:** Consider the responses provided by the Planning Commission and Medical Cannabis Commission (MCC) to Council's referral regarding the desired maximum number of Medical Cannabis Cultivation locations (Zoning Ordinance/BMC Section 23E.72.040.A) and give direction to staff regarding any recommended changes to the Zoning Ordinance.

**Financial Implications:** See report

Contact: Timothy Burroughs, Planning and Development, 981-7400

**Action:** M/S/C (Arreguin/Maio) to suspend the rules and extend the meeting to 11:30 p.m.

**Vote:** Ayes – Maio, Davila, Bartlett, Harrison, Hahn, Wengraf, Worthington, Arreguin; Noes – None; Abstain – Droste.

**Action:** 1 speaker. M/S/Failed (Hahn/Bartlett) to adopt the proposal from Councilmember Hahn in Supplemental Reports Packet #2

1. *To initially allow 6 Standard cultivation sites at no more than 22,000 square feet per site, as allowed by State regulations, for a cumulative maximum of 132,000 square feet. The remainder of square footage, up to a cumulative maximum of 182,000 square feet, would be dedicated to a Small Sites program, reserved for local, artisan, cooperative, and green growers, with 5 additional sites allowed, each of no more than 10,000 square feet. The total combined number of Standard and Small Sites allowed would be 11, and total square footage capped at 182,000 square feet;*
2. *To direct staff to create two application processes; one for Standard Sites and another for Small Sites favoring local, artisan, cooperative, and green growers;*
3. *To allow only 1 site per operator, and create an overall preference for qualified owners from populations or groups that are or have been disproportionately targeted for enforcement, criminalization, and/or incarceration related to marijuana offenses;*
4. *One year after a site commences operations, direct staff to undertake an evaluation that includes, but is not limited to, contacting neighbors and businesses within 500 feet and evaluating potential positive and negative impacts, recommending any helpful/necessary changes to the enabling code and helping ensure the operator is in compliance with all rules and regulations. This site-by-site review will be limited to 8 sites, representing a variety of sizes and locations, as a means of identifying benefits and challenges of cultivation operations and improving the City's regulatory framework;*
5. *Once the first 11 sites have been permitted, direct staff to evaluate the overall and cumulative success and impacts of the cultivation sites program on a neighborhood and city-wide basis, review the preferences and programs for effectiveness, and consider whether the number of sites can be increased.*

**Vote:** Ayes – Bartlett, Hahn; Noes – Davila, Harrison; Abstain – Maio, Wengraf, Worthington, Droste, Arreguin.

## Action Calendar – Old Business

**Action:** M/S/C (Harrison/Maio) to adopt the proposal from Councilmember Harrison in Supplemental Reports Packet #2 amended to include paragraph #3 from Councilmember Hahn's proposal.

*Direct staff to prioritize local growers and cooperatives in the permitting process or set aside some of the allotted square footage specifically for use by local small growers and cooperatives. This could be achieved by maintaining the limit of 6 cultivation locations between 15,000 and 22,000 ft<sup>2</sup> in size for all forms of cultivators (using between 90,000 and 132,000 of the available 180,000 ft<sup>2</sup>) while allocating the remaining 48,000 ft<sup>2</sup> to local cultivators and cooperatives, without a specific location limit. During the permitting process, each operator will be limited to one site to avoid anti-competitive practices and prevent a monopoly. After one year of operation, staff will evaluate the positive and negative impacts of the cultivation site on the surrounding businesses and neighbors, and enforce on a complaint-driven basis*

*#3 Hahn: To allow only 1 site per operator, and create an overall preference for qualified owners from populations or groups that are or have been disproportionately targeted for enforcement, criminalization, and/or incarceration related to marijuana offenses;*

**Vote:** Ayes – Maio, Davila, Bartlett, Harrison, Wengraf, Worthington, Droste, Arreguin; Noes – None; Abstain – Hahn.

**Action:** M/S/Failed (Droste/Wengraf) to adjourn the meeting.

**Vote:** Ayes – Maio, Bartlett, Wengraf, Droste; Noes – Davila, Harrison, Hahn, Worthington, Arreguin.

**Action:** M/S/C (Arreguin/Maio) to suspend the rules and extend the meeting to 12:00 a.m.

**Vote:** Ayes – Maio, Davila, Bartlett, Harrison, Hahn, Worthington, Arreguin; Noes – Droste; Abstain – Wengraf.



## Action Calendar – Old Business

36. **Analysis and Recommendations for the Pathways Project to Address Homelessness in Berkeley** *(Continued from June 27, 2017. Item contains supplemental materials.)*

**From: City Manager**

**Recommendation:** Prioritize funding decisions for proposed Pathways Project programs (an Encampment Resolution Team, a STAIR Center, a Bridge Living Community, and a Homeward Bound program) based on which homeless issue Council most wishes to address in Berkeley:

1. Fund an Encampment Resolution Team and a STAIR Center for an estimated \$2.4 million in year one, plus \$2.1 million annually thereafter, if Council most wishes to provide temporary respite for unsheltered homeless individuals with no dedicated housing exits.
2. Fund a Bridge Living Community and a Homeward Bound program for an estimated \$2.6 million in year one, plus \$2.4 million annually thereafter, if Council most wishes to house an estimated 100-120 homeless individuals per year, but add no new emergency respite programs.
3. Fund all four programs at an estimated \$4.8 million in year one, and an estimated \$4.3 million annually thereafter, if Council wishes to address both the goal of temporary respite and permanent housing concurrently.

All funding estimates include roughly \$190,000 for 1 FTE in new City Staff time for program administration.

The City Manager recommends prioritizing a Bridge Living Community and associated rental subsidies and a Homeward Bound program.

**Financial Implications:** See report

Contact: Paul Buddenhagen, Housing and Community Services, 981-5400

**Action:** M/S/C (Arreguin/Maio) to suspend the rules and extend the meeting to 12:15 a.m.

**Vote:** Ayes – Maio, Davila, Bartlett, Harrison, Hahn, Worthington, Arreguin; Noes – Droste; Abstain – Wengraf.

**Action:** 5 speakers. M/S/C (Hahn/Davila) to adopt “Option 4” as presented in the City Manager’s report to Council on June 27, 2017, submitted by Paul Buddenhagen, Director of Health, Housing and Community Services, to establish a combined STAIR Center/Bridge Living Community and associated Homeward Bound and rapid rehousing components with the following additions, as recommended by formal action of the Council’s Ad Hoc Subcommittee on Homelessness:

1. Add an Outreach Resolution Team
2. Add a program to address illegal dumping and excessive accumulations of items and materials associated with homeless encampments, in particular in the heavily impacted West Berkeley corridor

**Vote:** All Ayes.

## Action Calendar – Old Business

**37a. Allocation of U1 Funds by the City Council** *(Continued from June 27, 2017)*

**From: Housing Advisory Commission**

**Recommendation:** 1. As specified by Measure U1, the City Council shall receive and consider housing strategy recommendations from the Housing Advisory Commission prior to allocating any Measure U1 funds.

2. When considering allocations for U1 funds, the City Council will make specific findings of how the spending meets the goals of Measure U1: improve housing affordability in Berkeley and protect residents from homelessness.

**Financial Implications:** See report

Contact: Amy Davidson, Commission Secretary, 981-5400

**37b. Companion Report: Allocation of U1 Funds by the City Council** *(Continued from June 27, 2017)*

**From: City Manager**

**Recommendation:** 1. Reaffirm that, as specified in Measure U1, the City Council shall receive and consider recommendations by the Housing Advisory Commission on funding and programs to increase affordable housing and protect Berkeley residents from homelessness, either annually or biannually. 2. Take no action with regard to committing to make findings that expenditures meet the goals of Measure U1.

**Financial Implications:** See report

Contact: Jovan Grogan, Deputy City Manager, (510) 981-7000

**Action:** Item 37b moved to the Consent Calendar and approved recommendation as amended below.

*1. Reaffirm that the City Council shall receive and consider recommendations by the Housing Advisory Commission as specified in Measure U1; and 2. Take no action with regard to committing to make findings that expenditures meet the goals of Measure U1.*

**38a. Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley** *(Continued from June 27, 2017)*

**From: Housing Advisory Commission**

**Recommendation:** That the City Council not use U1 funds to backfill the Workers' Compensation Fund for the acquisition of the properties located at 1001, 1007, and 1011 University Avenue, and 1925 Ninth Street, City of Berkeley.

**Financial Implications:** See report

Contact: Amy Davidson, Commission Secretary, 981-5400

## Action Calendar – Old Business

- 38b. Companion Report: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley** *(Continued from June 27, 2017)*

**From: Housing Advisory Commission**

**Recommendation:** Accept staff's recommendation to use \$4,730,815 of Measure U1 revenue over a 5 year period (\$946,163 annually) to repay the Workers' Compensation Fund for the acquisition of the properties located at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley.

**Financial Implications:** See report

Contact: Jovan Grogan, Deputy City Manager, (510) 981-7000

**Action:** M/S/Failed (Hahn/Davila) to suspend the rules and extend the meeting to 12:25 a.m.

**Vote:** Ayes – Davila, Harrison, Hahn, Worthington, Arreguin; Noes – Maio, Bartlett, Wengraf; Abstain – None; Absent - Droste.

Councilmember Droste absent 12:05 a.m. – 12:15 a.m.

**Action:** 5 speakers. Item held over to July 25, 2017

## Action Calendar – New Business

- 39a. International Symbol of Accessibility (ISA) Change for City Signage**

**From: Commission on Disability**

**Recommendation:** Adopt a Resolution changing future signs indicating accessibility in Berkeley. The Berkeley Commission on Disability is recommending Council support a proposed change in signs that indicates accessibility.

**Financial Implications:** Minimal

Contact: Ella Callow, Commission Secretary, 981-6300

- 39b. Companion Report: International Symbol of Accessibility (ISA) Change for City Signage**

**From: City Manager**

**Recommendation:** Refer the item back to the Commission on Disability for further analysis regarding cost differences between the existing International Symbol of Accessibility signage and the recommended signage as well as specific vendors that currently provide the recommended signage to other municipalities.

**Financial Implications:** Unknown

Contact: Phillip Harrington, Public Works, 981-6300

**Action:** Item 39a moved to Consent Calendar. Adopted Resolution No. 68,095-N.S. changing future signs indicating accessibility in Berkeley.

## Action Calendar – New Business

### Information Reports

40. **FY 2018 Civic Arts Grant Awards**  
**From: City Manager**  
Contact: Jordan Klein, Economic Development, 981-7530  
**Action:** Received and filed.
41. **FY 2017 Investment Report: Quarter Ended March 31, 2017**  
**From: City Manager**  
Contact: Henry Oyekanmi, Finance, 981-7300  
**Action:** Received and filed.
42. **Status of City's \$6M Loan to the Ed Roberts Campus**  
**From: City Manager**  
Contact: Paul Buddenhagen, Housing and Community Services, 981-5400  
**Action:** Received and filed.
43. **Update on Retrofit Grants Program, Activities Funded by FEMA Hazard Mitigation Grant, and Status of the Soft Story Ordinance**  
**From: City Manager**  
Contact: Timothy Burroughs, Planning and Development, 981-7400  
**Action:** Received and filed.
44. **Status Report July 2017 - Audit of Equipment Replacement Reserve**  
**From: City Manager**  
Contact: Phillip Harrington, Public Works, 981-6300  
**Action:** Received and filed.

**Public Comment – Items Not Listed on the Agenda – 0 speakers.**

### Adjournment:

Adjourned at 12:15 a.m. in memory of:

1. Frances Rachel, Local Activist
2. David Williamson, Local Athlete and Mentor

### Communications

#### Restricting Flavored Tobacco Sales

1. Carol Denney

#### Vegetables Growing in Shade

2. Diego Aguilar-Canabal

#### Community Concerns

3. Nick Faber

**Housing and Climate Change**

4. Cameron Scherer

**Thank You Letter**

5. Berkeley Neighborhoods Council

**Housing and Zoning Suggestions**

6. Berkeley Design Advocates

**Berkeley Animal Care Services Concerns**

7. Jane Funk / Jovan Grogan

**Free Speech**

8. Therese Fitzpatrick (2)

**Environmental Health Division Concerns**

9. Leo Schwartz

**Bank Divestments**

10. Sheila Goldmacher

**Berkeley Police Department Response to Protest**

11. Rachel Lederman

**Bike Improvements for Repaving**

12. Dave Campbell

**Berkeley Rose Garden**

13. Annie Dillon

**Request for Certificate of Permissible Rent Level Form**

14. W.B.C.

**Supplemental Communications and Reports 1**

**Item 21: Referral to the Community Environmental Advisory Commission: Cigarette Butt Pollution Prevention Program in South Berkeley**

15. Revised materials, submitted by Councilmember Bartlett

**Item 24: Support of AB 214: Postsecondary Education, Student Hunger**

16. Revised materials, submitted by Councilmember Harrison

**Item 29: Housing Accountability Act**

17. Rob Wrenn

**Item 33: Expedited Review for Affordable Housing Projects**

18. Revised materials, submitted by Councilmember Hahn

**Item 35: Medical Cannabis Cultivation Ordinance Revisions**

19. Supplemental materials, submitted by Councilmember Hahn

**Item 36: Analysis and Recommendations for the Pathways Project to Address Homelessness in Berkeley**

20. Supplemental materials, submitted by Councilmember Hahn

**Item 37a: Allocation of U1 Funds by the City Council**

**Item 37b: Companion Report: Allocation of U1 Funds by the City Council**

**Item 38a: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

**Item 38b: Companion Report: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

21. Cecile Pineda
22. Norma Harrison
23. Tree Fitzpatrick
24. Nico Calavita

**Item 40: FY 2018 Civic Arts Grant Awards**

25. Bruce Coughran
26. Cherie Hill
27. Andrea Hirsig
28. Susan Muscarella
29. Andrew Page
30. Liz Ozol
31. Pamela Miller
32. Carol Lashof
33. Rebecca Seeman
34. George-Ann Bowers
35. Sara Gambina-Belknap
36. Janice Murota
37. Inferno Theatre
38. Dyana Vukovich
39. Sharon Dolan
40. Wendy Ponder
41. Emmerich Anklam
42. Rachel Nissim
43. Carol Handelman
44. Jan Zvaifler
45. Emily Wainacht

## **Supplemental Communications and Reports 2**

**Item 6: Housing Trust Fund Recommendation – Northern California Land Trust (NCLT) Scattered Site Rehabilitation**

46. Revised materials, submitted by Councilmember Harrison

**Item 13: Contract No. 9977 Amendment: Portable Computer Systems dba PCS Mobile to Purchase 15 Automated License Plate Recognition (ALPR) Units**

47. Alfred Twu
48. Ryan Thorngren

**Item 21: Referral to the Community Environmental Advisory Commission: Cigarette Butt Pollution Prevention Program in South Berkeley**

49. Carol Denney

**Item 25: Adopt a Resolution Approving the Allocation of \$3,131,651 in Predevelopment from the Housing Trust Fund for the Berkeley Way Project**

- 50. Revised materials, submitted by Councilmember Worthington
- 51. Supplemental materials, submitted by Health, Housing & Community Services

**Item 26: Support California AB 395 to Protect Internet Privacy**

- 52. Revised materials, submitted by Councilmember Worthington

**Item 27: Amending the Berkeley Election Reform Act to Implement Public Financing**

- 53. Daniel Newman, on behalf of the Berkeley Fair Elections Coalition
- 54. Rob Wrenn
- 55. Igor Tregub

**Item 28: Automatic Door Openers in Multi-Unit Residential**

- 56. Supplemental materials, submitted by Commission on Disability

**Item 32: Support the Resilient Shoreline Program of Citizens for East Shore Parks**

- 57. Revised materials, submitted by Mayor Arreguin

**Item 33: Expedited Review for Affordable Housing Projects**

- 58. Supplemental materials, submitted by Councilmember Droste

**Item 35: Medical Cannabis Cultivation Ordinance Revisions**

- 59. Supplemental materials, submitted by Councilmember Hahn
- 60. Supplemental materials, submitted by Councilmember Harrison
- 61. Medical Cannabis Commission
- 62. Charley Pappas

**Item 37a: Allocation of U1 Funds by the City Council**

**Item 37b: Companion Report: Allocation of U1 Funds by the City Council**

**Item 38a: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

**Item 38b: Companion Report: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

- 63. Sheila Goldmacher (2)
- 64. Lynnda Ohama
- 65. Jim Latchney
- 66. Christine Schwartz
- 67. Kris Eggen
- 68. Diana Bohn
- 69. Sally Nelson (2)
- 70. Bill Bogert
- 71. Judy Nakadegawa
- 72. Pei Wu
- 73. Joshua
- 74. Joel Reed
- 75. Daniel Moore
- 76. Joshua Pfeffer
- 77. Gary Hicks
- 78. Ellen Woods

- 79. Happy Skywalker
- 80. Pam Webster
- 81. Phil Allen
- 82. Marcia Poole
- 83. Lisa Giampaoli
- 84. Maurice Catlett
- 85. Norma Harrison
- 86. Moni Law
- 87. Cassidy Crofton
- 88. Linda Franklin
- 89. Chimey Lee
- 90. Lauren Chester
- 91. Alex White

**Item 25: Adopt a Resolution Approving the Allocation of \$3,131,651 in Predevelopment from the Housing Trust Fund for the Berkeley Way Project**

- 92. 37 Communications submitted via Berkeley Considers, includes summary information.

**Supplemental Communications and Reports 3**

**Item 6: Housing Trust Fund Recommendation – Northern California Land Trust (NCLT) Scattered Site Rehabilitation**

- 93. Ian Winters

**Item 13: Contract No. 9977 Amendment: Portable Computer Systems dba PCS Mobile to Purchase 15 Automated License Plate Recognition (ALPR) Units**

- 94. Presentation, submitted by Public Works Department
- 95. Gunnar Rieth
- 96. Felipe Diaz
- 97. Blair Beekman

**Item 27: Amending the Berkeley Election Reform Act to Implement Public Financing**

- 98. Presentation, submitted by Fair Campaign Practices Commission

**Item 35: Medical Cannabis Cultivation Ordinance Revisions**

- 99. Presentation, submitted by Planning & Development

**Item 36: Analysis and Recommendations for the Pathways Project to Address Homelessness in Berkeley**

- 100. Presentation, submitted by Health, Housing & Community Services

**Item 37a: Allocation of U1 Funds by the City Council**

**Item 37b: Companion Report: Allocation of U1 Funds by the City Council**

**Item 38a: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

**Item 38b: Companion Report: Use of U1 Funds for Property Acquisition at 1001, 1007, and 1011 University Avenue and 1925 Ninth Street, Berkeley**

- 101. Sheila Goldmacher
- 102. John Tortorice



**Misc. Communications**

**Board of Library Trustees**

103. Unknown

**HERO Program**

104. Unknown

DEPARTMENT ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

**SUBJECT: AUTOMATED LICENSE PLATE READER (ALPR)**

PURPOSE

- 1 - This order establishes guidelines for the use of the Berkeley Police Department's Automated License Plate Reader (ALPR) technology and data. ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR). ALPRs may be used by the Berkeley Police Department Parking Enforcement and Traffic Units for official law enforcement purposes.

POLICY

**Administration of ALPR Data**

- 2- Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain through the Traffic Bureau. The Investigations Division Captain will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

**ALPR Operation**

- 3- Department personnel shall not use, or allow others to use, the ALPR equipment or database records for any unauthorized purpose.
  - a. An ALPR shall only be used for official and legitimate law enforcement business.
  - b. Reasonable suspicion or probable cause is not required before using an ALPR.
  - c. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
  - d. No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

DEPARTMENT ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

**ALPR Data Collection and Retention**

- 4- All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.
- 5- The Parking Enforcement Manager is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by City Department of Information Technology personnel and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.
- 6- All ALPR data shall be stored as described in this order and thereafter shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data shall be downloaded from the server onto portable media and booked into evidence. The records will then be subject to standard evidence retention policies and statutes.
  - a. Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

**Accountability and Safeguards**

- 7- All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:
  - a. Non-law enforcement requests for access to stored ALPR data shall be processed according to General Order R-23 in accordance with applicable law.
  - b. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requestor is the registered owner of the vehicle in question, and when providing such

DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

- c. ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.
- d. Berkeley Police personnel approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- e. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only in connection with specific criminal investigations.
- f. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state, or federal agency or entity without the express written consent of the City Manager.
- g. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question.
- h. ALPR system audits will be conducted by personnel assigned to the Professional Standards Bureau on a regular basis, at least biennially.

**Current ALPR Deployments**

- 9- The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.
- 10- Effective 2/18/16, the Parking Enforcement Unit will utilize five (5) Parking Enforcement Go-4 vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV/SVS database (stolen and wanted vehicles). The

## DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

current contracted vendor for this system is PCS Mobile using Genetec ALPR technology.

- 11- The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and checks scanned "reads" against a file of vehicles which have five or more outstanding parking citations exceeding 30-days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the city to recover outstanding citation fees and penalties. ALPR equipment is installed in the Parking Enforcement Unit's Scofflaw Enforcement vehicle.
- 12- The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:
  - a. All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.
- 13- When a car is booted and/or towed, the read, hit, and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.
- 14- The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's goBerkeley parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner. The reports will provide only the date, time, location, approximate address, goBerkeley blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement

DEPARTMENTAL ORDER

ADMINISTRATIVE ORDER #001-2016

DATE ISSUED: 02/18/16

---

officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.



Michael K. Meehan  
Chief of Police

References: NCRIC ALPR Policy  
SB 34  
General Order R-23

Cc: All BPD Personnel

**EXPENDITURE NON-CONSTRUCTION CONTRACT REVIEW FORM: NEW CONTRACT**

CMS # XUHAL  
(To be filled in by department)

Contract # 9977  
(To be filled in by Auditor)

CONTRACTOR NAME: Portable Computer Systems dba PCS Mobile

Subject of Contract: License Plate Recognition System

This contract package contains:	Attached	Waiver Attached	Not Required
<b>3 Original Contracts (Department, Vital Record and Vendor) in folders</b>			
*The Vital Record contract MUST be in a folder. *Optional: In lieu of folders, Department and Vendor copies may be assembled with an Acco-fastener.			
1. CONTRACT BOILERPLATE <u>W/changes - see M. Woo e-mail</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2. Scope of Services (Exhibit <u>X</u> @ boilerplate) <u>Exhibit/Attachment B</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<del>3. Payment Provisions (Exhibit <u>X</u> @ boilerplate) <u>Attachment C</u></del>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4. Evidence of Competitive Solicitation OR Waiver by CM or by Council Resolution	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. CERTIFICATIONS <u>SPICK 14-10875-C</u>			
a. Workforce Composition (businesses with 5 or more employees)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Nuclear Free Berkeley Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
c. Oppressive States Disclosure (Exception: Community-based, non-profit organizations)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d. Certification of Compliance with Living Wage Ordinance (LWO): <u>use current form on web*</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e. Certification of Compliance with Equal Benefits Ordinance: <u>use current form on web*</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f. Community Agency: Certification of Anti-Lobbying	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. Community Agency: Certification of Drug-Free Workplace	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<del>6. Insurance Certificate/s AND Endorsement/s OR Insurance Waiver/s (originals, not copies)</del>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Authorizing Council Resolution # <u>66,917 1/27/15</u>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8. Consultant Contracts: Form 700, Statement of Economic Interests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<del>9. Federally Funded Project Requirement: Debarment status printout</del>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Berkeley Business License # BL-002930  
 Requisition # 185183 (Hard copy attached)  
 Budget Code 674 4920 431 30.38 11TD06  
840 4920 431 30.38 14TD01  
 Was there any advance payment? No  Yes  .....  
 30.38

Contract Amount \$ 450,000  
 Council Approved Amount \$ 450,000  
 If Yes, Advanced Amount \$ \_\_\_\_\_  
 If Yes, Purchase Order # \_\_\_\_\_

**Routing and signatures:**  
 All elements of the contract package, including information provided above, have been reviewed for completeness and accuracy and evidenced by the following signatures (Project Manager please print name):

1. WILLA NG / FARID JAVANDEL PW-TRANS 981-7061 6/11/15  
 Project Manager (PRINT NAME) & Department Phone No. Date

2. [Signature] 6/19/15  
 Department Administrative Officer/Accounting Date

3. [Signature] 6/19/15  
 Department Head Date

4. [Signature] 26 JUN 15  
 Contract Administrator Date

5. [Signature] 6/25/15  
 Budget Manager Date

Routing continues to the following persons, who sign directly on the contract:  
 6. City Manager (Will not sign unless all signatures and dates appear above)

**RECEIVED**  
 JUN 29 2015  
**CITY AUDITOR**

amh 6/29/15 JA 6/30/15

**LICENSE PLATE RECOGNITION SYSTEM SERVICES CONTRACT**

**THIS CONTRACT** is between the CITY OF BERKELEY ("City"), a Charter City organized and existing under the laws of the State of California, and Portable Computer Systems, Inc. dba PCS Mobile ("Provider"), a Colorado corporation doing business at 1200 W. Mississipp Avenue, Denver, Colorado, 80223, who agree as follows:

**Article 1. CONTRACT APPENDICES**

The Contract Appendices are as follows:

- A Security Center License Agreement
- B Scope of Services
- C Payment Terms
- D Equipment Specifications
- E Detailed Training Outline
- F Warranty Agreement and Software Maintenance Agreement
- G Equipment Acceptance Certificate
- H Current Police Administrative Order on use of aLPR Equipment

The terms of each of the appendices are incorporated herein by reference and made a part of this Contract. However, in the event of a conflict between any provision or term in this Contract and an Appendix, the terms of this Contract shall prevail.

**Article 2. SCOPE OF SERVICES**

Contractor agrees to perform all services described in Appendix A, Appendix B, Appendix E, Appendix F, Appendix G and Appendix H in accordance with its stated terms and conditions.

**Article 3. TERM AND RENEWAL**

3.1. The term of this contract shall be for a period of five (5) years. This Contract shall begin on May 1, 2015 and end on May 30, 2020. The City Manager of the City may extend the term of this contract by giving written notice.

3.2. The terms and conditions of this Contract shall not be altered or otherwise modified except by a written amendment to this Contract executed by City and Provider.

3.4. A written notice is deemed served when a party sends the notice in an envelope addressed to the other party to this Contract and deposits it with the U.S. Postal Service, first class mail, postage prepaid. For purposes of this Contract, all notices to City shall be addressed as follows:

City Manager  
City of Berkeley  
2180 Milvia Street  
Berkeley, California 94704

For purposes of this Contract, all notices to Provider shall be addressed as follows:

CMS# H04AL  
AUTH# 66917



Steve McKay, Treasurer, Manager of Finance  
Portable Computer Systems, Inc dba PCS Mobile  
1200 W. Mississippi Avenue  
Denver, CO 80233

3.5. If City terminates this Contract for convenience before Provider completes the services in Appendix B, Provider shall then be entitled to recover its costs expended up to that point plus a reasonable profit, but no other loss, cost, damage, expense or liability may be claimed, requested or recovered.

3.6. PCS Mobile warrants and represents that its officials, including its officers and employees in their official capacity, presently have no interest and agrees that its officials, including its officers and employees in their official capacity, will not acquire any interest which would represent a conflict of interest under California Government Code sections 1090 et seq. and 87100 et seq. during the performance of this Agreement.

**Article 4. PAYMENT TERMS**

4.1 For services referred to in Article 2 (Scope of Services), City will pay Provider a total amount not to exceed \$450,000. City shall make payments to Provider in accordance with the provisions described in Appendix C, which is attached to and made a part of this Contract.

**Article 5. PROVISIONS OF LICENSE PLATE RECOGNITION  
EQUIPMENT PURCHASE AND IMPLEMENTATION**

5.1. The license plate recognition ("LPR") equipment and software implementation will occur in accordance with the terms specified in Article 2 (Scope of Services).

5.2. Provider shall provide all required hosting and operations support for the System at costs identified in Appendix C.

5.3. Provider shall provide City a non-exclusive, non-transferable license to use the Hosted Software in accordance with the applicable documentation and in accordance with the terms set forth in Appendix A for the term of this Contract at a cost identified in Appendix C.

5.4. Provider shall provide five (5) LPR units, with specification described in Appendix D, to the City and provide all necessary City employees training as set forth in Appendix E to maintain this equipment for the term of this Contract.

5.5. Provider shall provide and perform the services in full compliance with all applicable laws, codes and standards (both public and private), including, but not limited to, the standards included in Appendix B and warranties expressed in Appendix F.

5.6. Provider shall provide goods for the term of this Contract as set forth in Appendix B.

5.7. Provider shall provide City technical support for the term of this Contract as set forth in Appendix B and Appendix F.

**Article 6. CITY'S RESPONSIBILITIES**

6.1. In connection with the performance of this contract and the provision of services, City shall be responsible for the following:

6.1.1 City shall be responsible for ensuring that City's use of the services and the performance of City's other obligations hereunder comply with all laws applicable to City.

6.1.2 City shall be responsible for the accuracy and completeness of all records and databases provided by City in connection with this Contract for use on Provider's system.

**Article 7. SUBCONTRACTING**

7.1. Provider is prohibited from subcontracting this Contract, or any part of it, unless such subcontracting is approved by City in advance in writing.

**Article 8. PROVIDER'S REPRESENTATIONS AND WARRANTIES**

In order to induce the City to enter into this Contract, Provider makes the following representations and warranties:

8.1. Provider has the expertise, manufacturing, management and maintenance capabilities, and financial capabilities to perform and complete all of its obligations contained in this Contract.

8.2. Provider is and will at all times be fully qualified and capable of performing its obligations under this Contract and possesses or will timely obtain all necessary licenses and/or permits required to perform such obligations.

8.3. Provider represents and agrees that the Services shall be performed in a professional manner and shall conform to established industry best practices.

8.4. Provider shall deliver all obligations undertaken in this Contract free and clear of all liens, rights of conditional vendors, encumbrances, and claims of copyright, patent or license holders, and in conformance with the requirements of this Contract.

**Article 9. INSURANCE**

9.1. Not less than ten (10) days prior to commencing any work, Provider shall furnish to City satisfactory proof that Provider has taken out for the entire period of this Contract the

following insurance in a form satisfactory to City and with an insurance carrier satisfactory to City, authorized to do business in California and rated by A.M. Best & Company A or better, which will protect those described below from claims described below which arise or are alleged to have arisen out of or result from the services of Provider, for which Provider may be legally liable, whether performed by Provider, its subcontractors or subconsultants of any tier or by those employed directly or indirectly by them or any of them, or by anyone for whose acts any of them may be liable. All insurance, except professional liability insurance, shall name the City, its officers, agents, volunteers and employees as additional insured's and shall provide primary coverage with respect to the City, and there shall be a waiver of subrogation as to each named and additional insured.

**9.1.1 Commercial general liability insurance:** Comprehensive or Commercial General Liability Insurance with limits not less than two million dollars (\$2,000,000.00) each occurrence Combined Single Limit for Bodily Injury and Property Damage, including Contractual Liability, Personal Injury, Products and Completed Operations. If the Comprehensive or Commercial General Liability Insurance is written on a Claims Made Form then, following termination of this Contract, coverage shall survive for a period of not less than five years. Coverage shall also provide for a retroactive date of placement coinciding with the effective date of this Contract.

**9.1.2 Professional liability insurance:** If any licensed professional performs services under this Contract, a professional liability insurance policy in the minimum amount of one million dollars (\$1,000,000.00) each occurrence to cover any claims arising out of Provider's performance of services under this Contract.

**9.1.3 Business automobile liability insurance:** Primary coverage shall be written on ISO Business Auto Coverage form CA 00 01 06 92 including symbol 1 (Any Auto), if applicable. Limits shall be not less than five hundred thousand dollars (\$500,000.00) each occurrence including coverage for owned, non-owned and hired vehicles, subject to a deductible of not more than ten thousand dollars (\$10,000.00) payable by Provider.

**9.1.4 Full workers' compensation liability insurance** for all persons whom Provider may employ in furnishing and providing the Services hereunder, in accordance with California law. Workers' compensation policy shall include Employer Liability Insurance with limits not less than one million dollars (\$1,000,000.00) each accident or occurrence. There shall be a waiver of subrogation as to the City and each named and additional insured under such policy.

9.2 Certificates of Insurance and Endorsements shall have clearly typed thereon the City contract number and title of contract, shall provide that the insurance carrier shall not cancel, terminate or otherwise modify the terms and conditions of said policies except upon thirty (30) days written notice to City's Contract Administrator. Endorsements naming the City as additional insured shall be attached to the Certificate of Insurance.

9.3 Nothing contained herein shall be construed as limiting in any way the extent to which Provider or any of its subcontractors or sub consultants may be held responsible for payment of damages resulting from their operations.

9.4 If Provider fails to maintain insurance, the City may take out insurance to cover any damages of the above mentioned classes for which the City and others to be insured referenced above might be held liable on account of Provider's failure to pay such damages, or compensation which the City might be liable under the provision of the Worker's Compensation Insurance and Safety Act, by reason of employee of Provider being injured or killed, and deduct, and in addition to any other remedy, retain amount of premium from any sums due Provider under this Contract.

9.5 Provider shall forward all insurance documents to:

**Department Name:** Public Works Transportation Division

**Attn:** Willa Ng

**CMS#** XUHAL

**Department Address:** 1947 Center Street, 3<sup>rd</sup> Floor, Berkeley, CA 94704

**Article 10. INDEMNIFICATION**

10.1 Provider shall indemnify, defend with counsel reasonably acceptable to the City, and hold harmless the City and its officials, commissioners, officers, agents, employees and volunteers from and against any and all loss, liability, claims, suits, actions, damages, injury (including, without limitation, injury to or death of an employee of Provider or its subcontractors), or any violation of any federal, state, or municipal law or ordinance, arising out of the willful misconduct or negligent acts or omissions of Provider or its employees, subcontractors, or agents, or by acts for which they could be held strictly liable, or by the quality or character of their work.

10.2 The foregoing obligation of Provider shall not apply when (a) the injury, loss of life, damage to property or violation of law arise wholly from the negligence or willful misconduct of the City or its officials, commissioners, officers, agents, employees and volunteers and (b) the actions of Provider or its employees, subcontractors, or agents have contributed in no part to the injury, loss of life, damage to property or violation of law. It is understood that the duty of Provider to indemnify and hold harmless includes the duty to defend as set forth in California Civil Code section 2778. Acceptance by City of insurance certificates and endorsements required under this Agreement does not relieve Provider from liability under this indemnification and hold harmless clause. This indemnification and hold harmless clause shall apply to any damages or claims for damages whether or not such insurance policies shall have been determined to apply. By execution of this Agreement, Provider agrees to the provisions of this Section and acknowledges that it is a material element of consideration.

**Article 11. CANCELLATION AND TERMINATION**

11.1 **Termination of Provider for Default.** In the event Provider fails to perform one or more of its material obligations under this Contract and has failed within twenty (20) days

of receiving notice from City to (a) cure the default or (b) if the default cannot be cured within twenty (20) days, provide the written assurances and plan as specified in subsection 11.1.1, this Contract may be terminated and all of Provider's rights hereunder ended. Termination will be effective after twenty (20) days written notice to Provider. No new work will be undertaken after the date of receipt of any notice of termination, or five (5) days after the date of the notice, whichever is earlier. In the event of such termination, Provider will be paid for those services performed under this Contract up to the date of termination and for reasonable direct costs incurred up to the date of termination, and any annual fees will be pro-rated. However, City may offset from any such amounts due Provider any damages or other costs City has or will incur due to Provider's non-performance. Any such offset by City will not constitute a waiver of any other remedies City may have against Provider for financial injury or otherwise.

11.1.1 If the City at any time reasonably believes that Provider is or may be in default under this Contract, the City may in its sole discretion notify Provider of this fact and request written assurances from Provider of performance of the Contract and a written plan from Provider to identify and attempt to remedy any failures to perform the terms of the Contract which the City may advise the Provider of in writing. Failure of the Provider to provide written assurances of performance as required herein will constitute a separate material breach of this Contract sufficient to invoke paragraph 11.1 above.

11.1.2 In the event a termination for cause is determined to have been made wrongfully or without cause, then the termination shall be treated as a termination for convenience in accordance with subsection 11.2, and Provider shall have no greater rights than it would have had if a termination for convenience had been effected in the first instance.

**11.2 Termination of Provider for Convenience.** Termination of this Agreement for convenience shall be in accordance with 49 C.F.R. 18.44.

11.2.1 City may terminate this Contract for City's convenience and without cause at any time by giving Provider thirty (30) days written notice of such termination. In the event of such termination, Provider will be paid for those services performed, pursuant to this Contract, up to the date of termination in accordance with Appendix C (Payment Terms). In no event will City be liable for costs incurred by Provider after receipt of notice of termination. Such non-recoverable costs include, but are not limited to, anticipated profits of this Contract, post-termination employee salaries, post-termination administrative expenses, or any other cost which is not reasonable or authorized under this section.

**11.3 Obligations of Provider Upon Termination.** Upon termination of this Contract, Provider will submit an invoice to City for an amount which represents the value of its work or services actually performed prior to the effective date of termination and for direct costs for which Provider is entitled under this Contract to be compensated, except that with respect to reimbursement for Provider's services, in no event will the compensation paid for the month in which the termination occurs be greater than the charges for the services delivered prior to the notice. Upon approval and payment of this invoice by City, City shall be under no further obligation to Provider monetarily or otherwise.

**11.4 Termination of City for Default.** City shall be in default of this Contract thirty (30) days after written notice of City's failure to comply in any respect with any material terms and conditions of this Contract and City fails to cure such breach within such thirty (30) day period. Notwithstanding the above, City shall be in default hereunder upon ten (10) business days written notice in the event the breach is due to non-payment by the City and City fails to cure such breach due to non-payment within such ten (10) day period.

**11.5 Return of City Data.** Within thirty (30) days of notification of termination of this Contract, Provider shall provide City with all City-owned data in dedicated data files suitable for importation into commercially available database software (e.g., MS-Access or MS-SQL). The dedicated data files will be comprised of City's data contained in Provider's system. The structure of the relational database will be specific to the City's data and will not be representative of the proprietary Provider's database.

## **Article 12. GENERAL WARRANTIES, LIMITATIONS ON WARRANTIES**

**12.1 Compliance with Specifications.** Provider's computer programs, files, hosted services, documentation and all other work product will strictly comply with the descriptions and representations made in Appendix D (Equipment Specifications) and including performance capabilities, completeness, specifications, configurations, and function that appear therein.

**12.2** Provider may lawfully grant the license set forth in Section 5.3 and Appendix A.

**12.3** Neither the licensed software or use of the hosted services, including all subsequent versions, updates, enhancements and/or releases, nor licensed materials, or the use thereof within the scope of the License, infringes a patent, trademark or copyright or is claimed to be a trade secret of any person who has not consented to the granting of the License. Developer shall indemnify and hold harmless City from and against any claims, including reasonable legal fees and expenses, based upon infringement of any United States copyright or patent by the Software. City agrees to notify Developer of any such claim promptly in writing and to allow Developer to control the proceedings. City agrees to cooperate fully with Developer during such proceedings. Developer shall defend and settle at its sole expense all proceedings arising out of the foregoing. In the event of such infringement, Developer may replace, in whole or in part, and at its own expense, the Software with a substantially compatible and functionally equivalent computer program or modify the Software to avoid the infringement.

**12.4** During the Initial Term, and any Renewal Term thereafter, the hosted services and software, including all subsequent versions, updates, enhancements and/or releases, will conform to the applicable printed documentation (i.e., all reference materials or manuals) delivered by Provider to City.

**12.5** Neither the software, including all subsequent versions, updates, enhancements and/or releases, nor the licensed materials or hosted services contain any virus, time bomb mechanism, or other software or code that can disable or adversely affect any and all of the software or the licensed materials or destroy any data or other software.

12.6 The limited warranty set forth in Section 12.1 is in lieu of all other warranties, express or implied warranties or merchantability and fitness for a particular purpose.

**Article 13. CONFORMITY WITH LAW AND SAFETY**

13.1 Provider shall observe and comply with all applicable laws, ordinances, codes and regulations of governmental agencies, including federal, state, municipal and local governing bodies having jurisdiction over any or all of the scope of services, including all provisions of the Occupational Safety and Health Act of 1979 as amended, all California Occupational Safety and Health Regulations, and all other applicable federal, state, municipal and local safety regulations. All services performed by Provider must be in accordance with these laws, ordinances, codes and regulations. Provider shall release, defend, indemnify and hold harmless City, its officers, agents, volunteers and employees from any and all damages, liability, fines, penalties and consequences from any noncompliance or violation of any laws, ordinances, codes or regulations.

13.2 If a death, serious personal injury or substantial property damage occurs in connection with the performance of this Contract, Provider shall immediately notify the City's Risk Manager by telephone. If any accident occurs in connection with this Contract, Provider shall promptly submit a written report to City, in such form as the City may require. This report shall include the following information: 1) name and address of the injured or deceased person(s); 2) name and address of Provider's subprovider, if any; 3) name and address of Provider's liability insurance carrier; and 4) a detailed description of the accident, including whether any of City's equipment, tools or materials were involved.

13.3 If a release of hazardous materials or hazardous waste that cannot be controlled occurs in connection with the performance of this Contract, Provider shall immediately notify the Berkeley Police Department and the City's Health Protection office.

13.4 Provider shall not store hazardous materials or hazardous waste within the City of Berkeley without a proper permit from the City.

**Article 14. NON-DISCRIMINATION**

14.1 Provider hereby agrees to comply with the provisions of Berkeley Municipal Code ("B.M.C.") Chapter 13.26 as amended from time to time. In the performance of this Contract, Provider agrees as follows:

14.2 Provider shall not discriminate against any employee or applicant for employment because of race, color, religion, ancestry, national origin, age (over 40), sex, pregnancy, marital status, disability, sexual orientation or AIDS.

14.3 Provider shall permit the City access to records of employment, employment advertisements, application forms, EEO-1 forms, affirmative action plans and any other documents which, in the opinion of the City, are necessary to monitor compliance with this non-discrimination provision. In addition, Provider shall fill-out, in a timely fashion, forms supplied by the City to monitor this non-discrimination provision.

**Article 15. INDEPENDENT CONTRACTOR**

15.1 Provider shall be deemed at all times to be an independent contractor and shall be wholly responsible for the manner in which Provider performs the services required of

Provider by the terms of this Contract. Provider shall be liable for its acts and omissions, and those of its employees and its agents. Nothing contained herein shall be construed as creating an employment, agency or partnership relationship between City and Provider.

15.2 Direction from City regarding the subject of this Contract shall be construed as providing for direction as to policy and the result of Provider's Work only and not as to the means or methods by which such a result is obtained.

15.3 Except as expressly provided in this Contract, nothing in this Contract shall operate to confer rights or benefits on persons or entities not party to this Contract.

15.4 Payment of any taxes, including California Sales and use Taxes, levied upon this Contract, the transaction, or the services or goods delivered pursuant hereto, shall be the obligation of Provider.

**Article 16. CONFLICT OF INTEREST PROHIBITED**

16.1 In accordance with Government Code section 1090, Berkeley City Charter section 36 and B.M.C. Chapter 3.64, neither Provider nor any employee, officer, director, partner or member of Provider, or immediate family member of any of the preceding, shall have served as an elected officer, an employee, or a City board, committee or commission member, who has directly or indirectly influenced the making of this Contract.

16.2 In accordance with Government Code section 1090 and the Political Reform Act, Government Code section 87100 *et seq.*, no person who is a director, officer, partner, trustee, employee or consultant of the Provider, or immediate family member of any of the preceding, shall make or participate in a decision made by the City or a City board, commission or committee, if it is reasonably foreseeable that the decision will have a material effect on any source of income, investment or interest in real property of that person or Provider.

16.3 Interpretation of this section shall be governed by the definitions and provisions used in the Political Reform Act, Government Code section 87100 *et seq.*, its implementing regulations, manuals and codes, Government Code section 1090, Berkeley City Charter section 36 and B.M.C. Chapter 3.64.

16.4 Provider shall disclose any financial, business, or other relationship with the City that may have an impact upon the outcome of this contract, or any ensuing City construction project. Provider shall also list current clients who may have a financial interest in the outcome of this contract, or any ensuing City construction project, which will follow.

16.5 Provider hereby certifies that it does not now have, nor shall it acquire any financial or business interest that would conflict with the performance of services under this contract.

16.6 Any subcontract in excess of \$25,000 entered into as a result of this contract, shall contain all of the provisions of this Article.

**Article 17. NUCLEAR FREE BERKELEY**

Provider agrees to comply with B.M.C. Chapter 12.90, the Nuclear Free Berkeley Act, as amended from time to time.



**Article 18. OPPRESSIVE STATES CONTRACTING PROHIBITION**

18.1 In accordance with Resolution No. 59,853-N.S., Provider certifies that it has no contractual relations with, and agrees during the term of this Contract to forego contractual relations to provide personal services to, the following entities:

- (1) The governing regime in any Oppressive State.
- (2) Any business or corporation organized under the authority of the governing regime of any Oppressive State.
- (3) Any individual, firm, partnership, corporation, association, or any other commercial organization, and including parent-entities and wholly-owned subsidiaries (to the extent that their operations are related to the purpose of its contract with the City), for the express purpose of assisting in business operations or trading with any public or private entity located in any Oppressive State.

18.2 For purposes of this Contract, the Tibet Autonomous Region and the provinces of Amdo, Kham, and U-Tsang shall be deemed oppressive states.

18.3 Provider's failure to comply with this section shall constitute a default of this Contract and City may terminate this Contract pursuant to Section 3. In the event that the City terminates Provider due to a default under this provision, City may deem Provider a non-responsible bidder for not more than five (5) years from the date this Contract is terminated.

**Article 19. RECYCLED PAPER FOR WRITTEN REPORTS**

If Provider is required by this Contract to prepare a written report or study, Provider shall use recycled paper for said report or study when such paper is available at a cost of not more than ten percent more than the cost of virgin paper, and when such paper is available at the time it is needed. For the purposes of this Contract, recycled paper is paper that contains at least 50% recycled product. If recycled paper is not available, Provider shall use white paper. Written reports or studies prepared under this Contract shall be printed on both sides of the page whenever practical.

**Article 20. BERKELEY LIVING WAGE ORDINANCE**

20.1 Provider hereby agrees to comply with the provisions of the Berkeley Living Wage Ordinance, B.M.C. Chapter 13.27. If Provider is currently subject to the Berkeley Living Wage Ordinance, as indicated by the Living Wage Certification form, attached hereto, Provider will be required to provide all eligible employees with City mandated minimum compensation during the term of this Contract, as defined in B.M.C. Chapter 13.27, as well as comply with the terms enumerated herein. Provider expressly acknowledges that, even if Provider is not currently subject to the Living Wage Ordinance, cumulative contracts with City may subject Provider to the requirements under B.M.C. Chapter 13.27 in subsequent contracts.

20.2 If Provider is currently subject to the Berkeley Living Wage Ordinance, Provider shall be required to maintain monthly records of those employees providing service under the Contract. These records shall include the total number of hours worked, the number of hours spent providing service under this Contract, the hourly rate paid, and the amount paid by Provider for health benefits, if any, for each of its employees providing services under the Contract. These records are expressly subject to the auditing terms described in Section 23.

20.3 If Provider is currently subject to the Berkeley Living Wage Ordinance, Provider shall include the requirements thereof, as defined in B.M.C. Chapter 13.27, in any and all

subcontracts in which Provider engages to execute its responsibilities under this Contract. All subprovider employees who spend 25% or more of their compensated time engaged in work directly related to this Contract shall be entitled to a living wage, as described in B.M.C. Chapter 13.27 and herein.

20.4 If Provider fails to comply with the requirements of this Section, the City shall have the rights and remedies described in this Section, in addition to any rights and remedies provided by law or equity.

Provider's failure to comply with this Section shall constitute a material breach of the Contract, upon which City may terminate this Contract pursuant to Section 3. In the event that City terminates Provider due to a default under this provision, City may deem Provider a non-responsible bidder for not more than five (5) years from the date this Contract is terminated.

In addition, at City's sole discretion, Provider may be responsible for liquidated damage in the amount of \$50 per employee per day for each and every instance of an underpayment to an employee. It is mutually understood and agreed that Provider's failure to pay any of its eligible employees at least the applicable living wage rate will result in damages being sustained by the City; that the nature and amount of the damages will be extremely difficult and impractical to fix; that the liquidated damage set forth herein is the nearest and most exact measure of damage for such breach that can be fixed at this time; and that the liquidated damage amount is not intended as a penalty or forfeiture for Provider's breach. City may deduct any assessed liquidated damages from any payments otherwise due Provider.

**Article 21. BERKELEY EQUAL BENEFITS ORDINANCE**

21.1 Provider hereby agrees to comply with the provisions of the Berkeley Equal Benefits Ordinance, B.M.C. Chapter 13.29. If Provider is currently subject to the Berkeley Equal Benefits Ordinance, as indicated by the Equal Benefits Certification form, attached hereto, Provider will be required to provide all eligible employees with City mandated equal benefits, as defined in B.M.C. Chapter 13.29, during the term of this contract, as well as comply with the terms enumerated herein.

21.2 If Provider is currently or becomes subject to the Berkeley Equal Benefits Ordinance, Provider agrees to provide the City with all records the City deems necessary to determine compliance with this provision. These records are expressly subject to the auditing terms described in Section 23 of this contract.

21.3 If Provider fails to comply with the requirements of this Section, City shall have the rights and remedies described in this Section, in addition to any rights and remedies provided by law or equity.

Provider's failure to comply with this Section shall constitute a material breach of the Contract, upon which City may terminate this contract pursuant to Section 3. In the event the City terminates this contract due to a default by Provider under this provision, the City may deem Provider a non-responsible bidder for not more than five (5) years from the date this Contract is terminated.

In addition, at City's sole discretion, Provider may be responsible for liquidated damages in the amount of \$50.00 per employee per day for each and every instance of violation of this Section. It is mutually understood and agreed that Provider's failure to provide its employees with equal benefits will result in damages being sustained by City; that the nature and amount of these damages will be extremely difficult and impractical to fix; that the liquidated damages

set forth herein is the nearest and most exact measure of damages for such breach that can be fixed at this time; and that the liquidated damage amount is not intended as a penalty or forfeiture for Provider's breach. City may deduct any assessed liquidated damages from any payments otherwise due Provider.

**Article 22. PREVAILING WAGES**

Certain labor categories under this contract may be subject to prevailing wages as identified in the State of California Labor Code commencing with Sections 1720 et. seq. and 1770 et. seq. These labor categories, when employed for any "work performed during the design and preconstruction phases of construction including, but not limited to, inspection and land surveying work," constitute a "Public Work" within the definition of Section 1720(a)(1) of the California Labor Code requiring payment of prevailing wages. In performing its obligations under this contract, Contractor is solely responsible to determine which, if any, of the work is governed by a labor category pursuant to California Labor Code sections 1720 et. seq. and 1770 et. seq. and pay the pertinent prevailing wage. Contractor shall defend, indemnify and hold harmless City concerning any liability arising out of Labor Code section 1720 et. seq. and 1770 et. seq.

**Article 23. AUDIT**

Pursuant to Section 61 of the Berkeley City Charter, the City Auditor's Office may conduct an audit of Provider's financial, performance and compliance records maintained in connection with the operations and services performed under this Contract. In the event of such audit, Provider agrees to provide the City Auditor with reasonable access to Provider's employees and make all such financial, performance and compliance records available to the Auditor's Office. City agrees to provide Provider an opportunity to discuss and respond to any findings before a final audit report is filed.

**Article 24. AMENDMENTS**

The terms and conditions of this Contract shall not be altered or otherwise modified except by a written amendment to this Contract executed by City and Provider.

**Article 25. CITY BUSINESS LICENSE, PAYMENT OF TAXES, TAX I.D. NUMBER**

Provider has obtained a City business license as required by B.M.C. Chapter 9.04, and its license number is written below; or, Provider is exempt from the provisions of B.M.C. Chapter 9.04 and has written below the specific B.M.C. section under which it is exempt. Provider shall pay all state and federal income taxes and any other taxes due. **Provider certifies under penalty of perjury that the taxpayer identification number written below is correct.**

Business License Number BL-002930  
Taxpayer ID Number 84-1396969

**Article 26.****MISCELLANEOUS**

**26.1 Governing Law.** This Contract shall be deemed to have been executed in Alameda County. The formation, interpretation and performance of this Contract shall be governed by the laws of the State of California, excluding its conflict of laws rules. Venue for all litigation relative to the formation, interpretation and performance of this Contract shall be in Alameda County, California.

**26.2 Assignment.** Neither City nor Provider shall assign this Contract without the prior written consent of the other party and any purported assignment without the other party's consent shall be void.

**26.3 Compliance with Applicable Laws.** Provider and any subcontractors shall comply with all laws, including the Berkeley City Charter, the Berkeley Municipal Code, and all city policies, rules and regulations which are applicable to the performance of the Services hereunder.

**26.4 Severability.** If a court of competent jurisdiction finds or rules that any provision of this Contract is invalid, void, or unenforceable, the provisions of this Contract not so adjudged shall remain in full force and effect. The invalidity in whole or in part of any provision of this Contract shall not void or affect the validity of any other provision of this Contract.

**26.5 No Implied Waiver of Breach.** The waiver of any breach of a specific provision of this Contract does not constitute a waiver of any other breach of that term or any other term of the contract.

**26.6 Solicitation.** Provider agrees not to solicit business at any meeting, focus group, service call, or interview related to this Contract, either orally or through any written materials.

**26.7 Force Majeure.** Neither party shall be in default or otherwise liable for any delay in or failure of its performance under this Contract if such delay or failure arises by any reason beyond its reasonable control, including any act of God, any acts of the common enemy, the elements, earthquakes, floods, fires, epidemics, riots, or acts of terrorism, provided, however, that lack of funds shall not be deemed to be a reason beyond a party's reasonable control. The parties will promptly inform and consult with each other as to any of the above causes which in their judgment may be the cause of a delay in the performance of this Contract.

**26.8 Integration, Incorporation:** This Contract, including all of the Appendices attached hereto, represents the entire and integrated Contract between City and Provider and supercedes all prior negotiations, representations, or Contracts, either written or oral. All exhibits attached hereto are incorporated by reference herein.

**26.9 Counterparts.** This Contract may be executed in multiple counterparts, each of which shall be an original and all of which together shall constitute one Contract.

26.10 **Contract Administration.** This Contract shall be administered by Danette Perry, Parking Services Manager, Public Works Department, or her designee, who shall act as the City's representative. All correspondence shall be directed to or through Ms. Perry or her designee.

26.11 **Section Headings.** The sections and other headings of this Contract are for convenience of reference only and shall be disregarded in the interpretation of this Contract

26.12 **Notices.** Any written notice to the City shall be sent to:

Farid Javandel  
Public Works Department  
City of Berkeley  
1947 Center Street  
Berkeley, California 94704

Any written notice to Provider shall be sent to:

Steve McKay, Treasurer, Manager of Finance,  
Portable Computer Systems, Inc dba PCS Mobile  
1200 W. Mississippi Avenue  
Denver, Colorado, 80223

Article 27. **FEDERAL REQUIREMENTS**

27.1 **CONFLICT OF INTEREST**

- A. Provider shall disclose any financial, business, or other relationship with the City that may have an impact upon the outcome of this contract, or any ensuing City construction project. Provider shall also list current clients who may have a financial interest in the outcome of this contract, or any ensuing City construction project, which will follow.
- B. Provider hereby certifies that it does not now have, nor shall it acquire any financial or business interest that would conflict with the performance of services under this contract.
- C. Any subcontract in excess of \$25,000 entered into as a result of this contract, shall contain all of the provisions of this Article.

27.2 **REBATES, KICKBACKS OR OTHER UNLAWFUL CONSIDERATION (Verbatim)**

Provider warrants that this contract was not obtained or secured through rebates kickbacks or other unlawful consideration, either promised or paid to any CITY employee. For breach or violation of this warranty, CITY shall have the right in its discretion; to terminate the contract without liability; to pay only for the value of the work actually performed; or to deduct from the contract price; or otherwise recover the full amount of such rebate, kickback or other unlawful consideration.

27.3 **PROHIBITION OF EXPENDING CITY STATE OR FEDERAL FUNDS FOR LOBBYING**

- A. Provider certifies to the best of his or her knowledge and belief that:
  - 1. No state, federal or City appropriated funds have been paid, or will be paid by-or-on behalf of Provider to any person for influencing or attempting to influence an officer or

employee of any state or federal agency; a Member of the State Legislature or United States Congress; an officer or employee of the Legislature or Congress; or any employee of a Member of the Legislature or Congress, in connection with the awarding of any state or federal contract; the making of any state or federal grant; the making of any state or federal loan; the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any state or federal contract, grant, loan, or cooperative agreement.

2. If any funds other than federal appropriated funds have been paid, or will be paid to any person for influencing or attempting to influence an officer or employee of any federal agency; a Member of Congress; an officer or employee of Congress, or an employee of a Member of Congress; in connection with this federal contract, grant, loan, or cooperative agreement; Provider shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.

B. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

C. Provider also agrees by signing this document that he or she shall require that the language of this certification be included in all lower-tier subcontracts, which exceed \$100,000 and that all such sub recipients shall certify and disclose accordingly.

#### 27.4 STATEMENT OF COMPLIANCE

Provider's signature affixed herein, and dated, shall constitute a certification under penalty of perjury under the laws of the State of California that Provider has, unless exempt, complied with, the nondiscrimination program requirements of Government Code Section 12990 and Title 2, California Administrative Code, Section 8103.

During the performance of this Contract, Provider and its subProviders shall not unlawfully discriminate, harass, or allow harassment against any employee or applicant for employment because of sex, race, color, ancestry, religious creed, national origin, physical disability (including HIV and AIDS), mental disability, medical condition (e.g., cancer), age (over 40), marital status, and denial of family care leave. Provider and subProviders shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. Provider and subProviders shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12990 (a-f) et seq.) and the applicable regulations promulgated there under (California Code of Regulations, Title 2, Section 7285 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations, are incorporated into this Contract by reference and made a part hereof as if set forth in full. Provider and its subProviders shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other Agreement.

The Provider shall comply with regulations relative to Title VI (nondiscrimination in federally-assisted programs of the Department of Transportation – Title 49 Code of Federal Regulations, Part 21 - Effectuation of Title VI of the 1964 Civil Rights Act). Title VI provides that the recipients of federal assistance will implement and maintain a policy of nondiscrimination in which no person in the state of California shall, on the basis of race, color, national origin, religion, sex, age, disability, be excluded from participation in, denied the benefits of or subject to discrimination under any program or activity by the recipients of federal assistance or their assignees and successors in interest.

The Provider, with regard to the work performed by it during the Agreement shall act in

accordance with Title VI. Specifically, the Provider shall not discriminate on the basis of race, color, national origin, religion, sex, age, or disability in the selection and retention of SubProviders, including procurement of materials and leases of equipment. The Provider shall not participate either directly or indirectly in the discrimination prohibited by Section 21.5 of the U.S. DOT's Regulations, including employment practices when the Agreement covers a program whose goal is employment.

#### 27.5 DEBARMENT AND SUSPENSION CERTIFICATION

A. Provider's signature affixed herein, shall constitute a certification under penalty of perjury under the laws of the State of California, that Provider has complied with Title 2 CFR, Part 180, "OMB Guidelines to Agencies on Government wide Debarment and Suspension (nonprocurement)", which certifies that he/she or any person associated therewith in the capacity of owner, partner, director, officer, or manager, is not currently under suspension, debarment, voluntary exclusion, or determination of ineligibility by any federal agency; has not been suspended, debarred, voluntarily excluded, or determined ineligible by any federal agency within the past three (3) years; does not have a proposed debarment pending; and has not been indicted, convicted, or had a civil judgment rendered against it by a court of competent jurisdiction in any matter involving fraud or official misconduct within the past three (3) years.

Any exceptions to this certification must be disclosed to CITY.

B. Exceptions will not necessarily result in denial of recommendation for award, but will be considered in determining Provider responsibility. Disclosures must indicate to whom exceptions apply, initiating agency, and dates of action.

C. Exceptions to the Federal Government Excluded Parties List System maintained by the General Services Administration are to be determined by the Federal highway Administration.

#### 27.6 CONTINGENT FEE

Provider warrants, by execution of this contract that no person or selling agency has been employed, or retained, to solicit or secure this contract upon an agreement or understanding, for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees, or bona fide established commercial or selling agencies maintained by Provider for the purpose of securing business. For breach or violation of this warranty, City has the right to annul this contract without liability; pay only for the value of the work actually performed, or in its discretion to deduct from the contract price or consideration, or otherwise recover the full amount of such commission, percentage, brokerage, or contingent fee.

#### 27.7 INSPECTION OF WORK

Provider and any subconsultant shall permit City, the state, and the FHWA if federal participating funds are used in this contract; to review and inspect the project activities and files at all reasonable times during the performance period of this contract including review and inspection on a daily basis.

#### 27.8 NATIONAL LABOR RELATIONS BOARD CERTIFICATION

In accordance with Public Contract Code Section 10296, Provider hereby states under penalty of perjury that no more than one final unappealable finding of contempt of court by a federal court has been issued against Provider within the immediately preceding two-year period, because of Provider's failure to comply with an order of a federal court that orders Provider to comply with an order of the National Labor Relations Board.

#### 27.9 ACCESS TO RECORDS

A. In accordance with 49 C.F.R. 18.36(i), the Provider agrees to provide the CITY, the FHWA, the Comptroller General of the United States or any of their authorized representatives access to any books, documents, papers and records of the Provider which are directly

pertinent to this contract for the purposes of making audits, examinations, excerpts and transcriptions.

B. The Provider agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

C. The Providers agrees to maintain all books, records, accounts and reports required under this contract for a period of not less than three years after the date of termination or expiration of this contract, except in the event of litigation or settlement of claims arising from the performance of this contract, in which case Contractor agrees to maintain same until the CITY, FHWA, the Comptroller General, or any of their duly authorized representatives, have disposed of all such litigation, appeals, claims or exceptions related thereto. Reference 49 CFR 18.39(i)(11).



IN WITNESS WHEREOF, City and Provider have executed this Contract as of the date written on the first paragraph of this Contract.

FOR CITY OF BERKELEY

Signed by:

\_\_\_\_\_  
*Christine Del*  
City Manager

Countersigned by:

\_\_\_\_\_  
*Ann Marie Hogan 6/29/15*  
City Auditor

Approved as to form by:

\_\_\_\_\_  
*Michael Woo*  
City Attorney for City of Berkeley

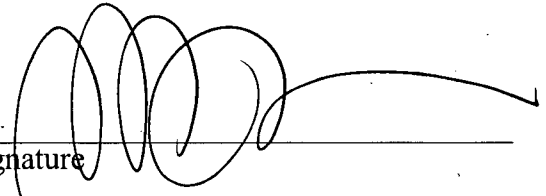
Attested by:

\_\_\_\_\_  
*Rose Hansen*  
Dep City Clerk

Provider

Portable Computer Systems Inc  
~~DA~~ PCS Mobile

Provider Name (print or type)



Signature

Martin Murphy

Print Name

Vice-President

Tax Identification



Berkeley Business License # BL-002930

Incorporated: Yes  No

Certified Woman Business Enterprise: Yes No

Certified Minority Business Enterprise: Yes No

If yes, state ethnicity: \_\_\_\_\_

Certified Disadvantaged Business Enterprise: Yes No

**TABLE OF APPENDICES**

Appendix	Title
A	SECURITY CENTER LICENSE AGREEMENT
B	SCOPE OF SERVICES
C	PAYMENT TERMS
D	EQUIPMENT SPECIFICATIONS
E	DETAILED TRAINING OUTLINE
F	WARRANTY AGREEMENT
G	SOFTWARE MAINTENANCE & SUPPORT AGREEMENT
H	EQUIPMENT ACCEPTANCE CERTIFICATE
I	CURRENT POLICE ADMINISTRATIVE ORDER ON USE OF ALPR

## APPENDIX A

SECURITY LICENSE AGREEMENT?

This Appendix A is attached to and incorporated by reference in the Contract made May 1, 2015 between the CITY OF BERKELEY ("City") and Portable Computer Systems, Inc. dba PCS Mobile, ("Provider"), providing for the licensing and services related to License Plate Recognition Equipment and Software purchase.

**1 GRANT OF LICENSE**

- 1.1 Provider grants City a non-exclusive and non-transferable license for the term of this Contract to use the systems software that is hosted by Provider and described below in subsection 1.4.
- 1.2 **Licensed Content, Not City Owned:** Nothing in this Agreement will be construed as assigning, selling, conveying, or otherwise transferring any ownership rights or title in Genetec AutoVu , including but not limited to pre-existing or independently developed intellectual property, materials, software, methodologies, tools, or inventions, that are developed, conceived or created for any Genetec business purpose, or any derivative works to any of the foregoing.
- 1.3 **City Purchased Equipment:** Nothing in this agreement will be construed as assigning, selling, conveying, or otherwise transferring any intellectual property ownership rights in Genetec Equipment including but not limited to pre-existing or independently developed intellectual property materials, software, methodologies, tools, or inventions, that are developed, conceived or created for any PCS MOBILE / GENETEC business purpose, or any derivative works to any of the foregoing.

**2 RESTRICTIONS ON USE**

City is authorized to use the Software hosted by Provider only for City's internal purposes. City agrees that it will not use or permit the Software to be used by any other entity.

**3 DATA OWNERSHIP AND RESPONSIBILITIES**

- 3.1 Provider shall be responsible for providing all equipment and software necessary for maintaining all data files. Data files are expressly the property of the City of Berkeley. Additionally, data files shall be readily transferable to new systems that the City may choose to use in the future.
- Microsoft SQL Server (MSSQL) is the City's preferred Relational Data Base Management

System. The City is currently standardized on MSSQL 2008 R2, but has begun implementing MSSQL 2012 and MSSQL 2014.

- 3.2 Provider agrees that it shall not at any time sell, assign, transfer or otherwise make available to, or allow use by Provider, agent of Provider or a third party any of the City's Proprietary Information.
- 3.3 Provider shall hold in confidence the City's Proprietary Information and allow its employees access to City's data only for the purposes of complying with this Contract.
- 3.4 Provider will take all necessary measures to secure and protect City's data including, but not limited to, daily backups, offsite storage of backup media, graphics, physical security, software access controls, encryption and proper backup rotations. Provider acknowledges that City is entitled to copy, export or otherwise duplicate City's data at any time.
- 3.5 Provider will maintain data security protocols that match or exceed safeguards for data use, storage, access and archive stated in the Berkeley Police Departments' most current Administrative or General Order on the use of Automatic LPR equipment and software. The Police Departments' current Administrative Order is incorporated by reference in this section, and included in Appendix H.
- 3.6 The provisions of this section (Data Ownership and Responsibilities) of the Contract shall survive expiration or termination of this Contract.

END OF APPENDIX A

**APPENDIX B**

**SCOPE OF SERVICES**

This Appendix B is attached to and incorporated by reference in the Contract made May 1, 2015 between the CITY OF BERKELEY ("City") and Portable Computer Systems, Inc. dba PCS Mobile., ("Provider"), providing for the License Plate Recognition Equipment and Software purchase.

**1 Deliverables**

Provider shall provide the City with complete product, installation, and training associated with delivering a License Plate Recognition Equipment and Software System.

**DEFINITIONS:**

- 1.1.LPR: The term "LPR" or "license plate recognition" refers to equipment and software that detects the presence of a vehicle and reports the numbers and letters shown on the license plate.
- 1.2.mLPR: The term "mLPR" shall mean "mobile license plate recognition", are units specifically designed for mounting on a vehicle for detection of vehicles while in motion.
- 1.3.LPR system: The term "LPR system" shall refer to all components for an operational system, including the mLPR external and in-vehicle equipment, operating software, data storage systems and data transmission equipment and software and integration equipment and software.
- 1.4.Days: The term "Day(s)" shall mean calendar days and not business or working days, unless otherwise indicated.
- 1.5.Contract Manager: The term "Contract Manager" shall mean the City employee responsible for the coordination with the Provider for the implementation, operation and management of the LPR system and for the City's day-to-day administration and coordination of City responsibilities for the LPR system pursuant to the contract.
- 1.6.Parking Occupancy: The term "parking occupancy" refers to the number of vehicles parked on a blockface, block, street segment or area, by date and time.
- 1.7.Time Limit Violation: The term "time limit violation" shall be defined as any vehicle that has been parked longer than the time limit posted by the parking sign or parking meter that governs that space, unless the vehicle displays a valid permit for that space.

- 1.8. Automatic Data Collection System: The term "Automatic Data Collection System" refers to the system by which the City collects and summarizes parking occupancy data for the purposes of analysis and setting rate and time limit policies.
- 1.9. Functional LPR. The term "Functional LPR" shall mean any of the Provider's mLPR units functioning within the normal parameters of operation. A Functional LPR will detect and report vehicle license plates, report vehicles that match criteria input by the operator, e.g. time limit violations, create summary reports and integrate with the City's Automatic Data Collection System and police enforcement systems. Acceptance of the mLPR unit by the City shall be based on the mLPR unit being a fully Functional LPR.
- 1.10. Acceptance: The term "Acceptance" shall mean the point at which the City assumes responsibility for payment of merchandise provided by the Provider. Acceptance shall occur after the City has successfully installed the equipment and the equipment is properly integrated and communicating with the City's Automatic Data Collection System and enforcement systems. mLPR units must meet the definition of Functional LPR at the time of acceptance.

## **2 PROVIDER'S RESPONSIBILITIES**

- 2.1. Provider shall deliver and install a Functional LPR, and provide an external web-based system to which the mLPR units connect and provide services to the City of Berkeley in accordance with the terms of this Agreement. The items, quantities, descriptions and unit prices that PCS MOBILE will provide under this contract are listed in Appendix C Payment Terms.
- 2.2. The provider's technology shall conform to the following standards:
- Security protocols that meet or exceed the standards set in Appendix H.
  - All applicable local, state and federal guidelines and laws.
- 2.3. Provider shall deliver and install equipment and software for five (5) operational mLPR units on City vehicles that range in size from the Go-4 parking enforcement vehicle to an SUV type vehicle. All equipment is to be new and fully tested and perform according to the specifications provided and described in Appendix D of this Agreement.
- 2.4. Provider shall develop customized software for use of the Functional LPR to collect parking occupancy data, including complete integration to the City's Automatic Data Collection System.
- 2.5. Provider shall provide and maintain an external data storage and web-based service to integrate with the City's Automatic Data Collection System.

**3 SUPPORTIVE SERVICES**

3.1 Provider shall provide the following additional services in conjunction with this Agreement:

- 3.1.1 Pre-delivery, detailed training and preparation of City's staff as detailed in Appendix E and as required for the following:
- 3.1.2 Installation of mLPR units on City's GO-4 vehicles;
- 3.1.3 Maintenance activities;
- 3.1.4 Troubleshooting problems;
- 3.1.5 Operations- programming, inventory, etc.:

3.1 During the term of this agreement, the Provider shall provide the following services:

**3.2.1 SERVICE DESCRIPTIONS**

<u>Ref. No.</u>	<u>Service Name</u>	<u>Description</u>	<u>Specifications</u>
1.	Maintenance - Phone Support	This is a service that will give the Customer a tool for technical support, but the Customer will apply the fix. When an issue develops, the Customer can call a PCS Mobile technician and the technician will help the Customer troubleshoot the problem over the phone.	Shall be initiated only by Customer's Designated Representative. Phone support shall support English language. Incidents (Tickets) will be tracked in AutoTask for every issue. One of the tools PCS Mobile may use is a remote session to the computer of the affected unit to determine and address problem.
2.	Maintenance -On-Site Support	Any service or support that requires a PCS Mobile technician to go to the Customer site to resolve the issue. This service will be provided on an as needed and determined basis by the City of Berkeley exclusively.	Tickets will be tracked in AutoTask for every issue. Types of issues <ul style="list-style-type: none"> <li>• Mounting Issues: Issues where the mount needs to be addressed to resolve a safety concern.</li> <li>• Data Issues: Issues where the data solution is not working. This can be a connectivity issue or device failure.</li> <li>• Power Issues: Issues where the 12v power/wiring, power distribution is an issue.</li> </ul>



			<ul style="list-style-type: none"> <li>• Camera issues: Issues where the camera is not reading properly, etc. Must be a new issue or change in a known good operating solution. (Troubleshooting) Visits can be scheduled to handle a list of issues or for Preventative Maintenance (PM).</li> </ul>
3.	Depot Repair (Warranty)	This is a service where any hardware warranty issues are issued to PCS Mobile. The PCS Mobile technician will troubleshoot/verify the problem and facilitate the repair through the manufacturer, on behalf of the Customer.	<p>Ticket will be tracked in AutoTask for every issue.</p> <p>Equipment must be covered under the Manufacturer's Warranty.</p> <p>PCS Mobile must have physical possession of Equipment.</p> <p>Can be picked up by PCS Mobile representative or, can be shipped to PCS Mobile facility.</p> <p>PCS Mobile will set up Return Manufacturer Approval RMA with manufacturer.</p> <p>PCS Mobile will prepare the equipment to be shipped per manufacturer instructions.</p> <p>PCS Mobile will receive repaired/replaced equipment and deliver to customer.</p> <p>Warranty repair service history will be tracked and reported.</p>
4.	Spares	Spare equipment specifications have been provided in Appendix C.	
5.	Preventative Maintenance	<p>Service consisting of testing individual components to assist in the prevention of failure.</p> <p>Purpose of preventative maintenance is to stay ahead of any potential issues in the Customer's mobile environment.</p> <p>PCS Mobile will provide one (1) Preventative Maintenance visit for each of 5 mLPR units deployed per 6 months.</p>	<p>Work will be performed on-site.</p> <p>All preventative maintenance will be documented in an AutoTask Ticket so that proper reporting can be delivered to customer and to internal staff.</p> <p>Preventative Maintenance work shall include:</p> <ul style="list-style-type: none"> <li>• Checking mounting equipment – sturdiness, torque on bolts, general wear and tear, etc.</li> <li>• MDC quick hardware diagnostics – this is a pass/fail test on the internal hardware components.</li> <li>• Video processor diagnostics.</li> <li>• Camera diagnostics.</li> <li>• Checking mounting of cameras.</li> <li>• Verification of proper termination, voltage and containment of all wiring.</li> <li>• Inventory of all mobile data, video and</li> </ul>

			<ul style="list-style-type: none"> <li>mounting equipment.</li> <li>General cleaning of external surfaces of devices.</li> <li>Reporting features of work done, which can include preventative maintenance history, listing of common problems to determine failure rates.</li> <li>Minor adjustments and/or fixes.</li> </ul>
--	--	--	--

3.2.2 SERVICE MANAGEMENT

3.2.2.1 SERVICE AVAILABILITY

Ref. No.	Service Name	Availability	Response	Restrictions
1.	Maintenance - Phone Support	8 to 5 Pacific Standard Time, business days (Normal Working Hours).	PCS Mobile will respond to phone call and/or phone message within 30 minutes.	
2.	Maintenance - On-Site Support	8 to 5 Pacific Standard Time, business days (Normal Working Hours).	PCS Mobile will respond as quickly as determined necessary by the City of Berkeley while keeping travel costs in mind.  Visits can be scheduled to handle a list of issues or for Preventative Maintenance	PCS
3.	Depot Repair (Warranty)	8 to 5 Pacific Standard, business days (Normal Working Hours).	PCS Mobile will process return to Manufacturer repair facility within one (1) business day.	Repair and return limited to manufacturer's response.
4.	Spares	8 to 5 Pacific Standard, business days (Normal Working Hours).	Spare parts may be replaced through purchase by the City of Berkeley. The spare parts will be used to supplement the extended warranty and to maximize uptime of systems.	
5.	Preventative Maintenance	8 to 5 Pacific Standard, business days (Normal Working Hours).	Preventative maintenance time frames will average 2-3 hours, depending on services offered. This service will be provided when directed exclusively by the City of Berkeley.	

3.2.2.2 SERVICE REQUESTS

In support of services outlined in this Agreement, the Customer may place service requests with PCS Mobile by phone or email. PCS Mobile will respond to service related incidents and/or requests submitted by the Customer within time frames as indicated under Service Availability/Response.

3.2.2.3 SERVICE REPORTING

Ref. No.	Report Name	Report Description	Report Interval	Recipient
1.	Support Ticket History Report	Custom reporting. Support history provided with detail for any time period as determined in agreement. Report would cover all activity as indicated in support activity: Phone Support, On-Site, Depot Repair, Spare Usage.	Monthly	
2.	Preventative Maintenance Report	Report features of work done, which can include preventative maintenance history and listing of common problems to determine failure rates.	Monthly	

3.3 ADDITIONAL SERVICES

If substantial changes in any Services are required due to reasons beyond the control of the Provider, such changed Services shall be considered Additional Services and additional fees may be required. Any such changed Services will be performed only if approved by City prior to beginning of work thereon, and will be invoiced as Additional Services at the rates indicated in the table HOURLY BILLING RATES.

City further agrees to pay PCS Mobile for any Additional Services promptly upon receipt of invoice therefore. City will also reimburse PCS Mobile, promptly upon receipt of invoice, for any and all out-of-pocket expenses incurred by PCS Mobile in the performance of Additional Services.

## HOURLY BILLING RATES

Technician Level	Hourly Billing Rate
Field Service Representative I	\$65
Field Service Representative II	\$75
Field Service Representative III	\$90
Video/LPR Specialist	\$125
Software Engineer / Database Technician	\$156.25

3.4 Integration and data storage, transmission that meets the standards of the City's Automatic Data Collection System with requirements as shown in Appendix D. City customization requests may incur additional costs that will be quoted and approved by the City prior to commencement of such project.

3.6 Provider will offer all available mLPR software upgrades, including those developed for other customers, at no additional charge to the City. City shall maintain the sole authority to determine when and where such upgrades will be implemented. Additional charges may apply for new software that requires new or upgraded hardware.

3.7 All data related to the LPR system will be maintained by the Provider and replicated on one or more duplicate servers with periodic backups. Further redundancy will be provided by replicating the data daily on a secure server located within the continental United States. Data will be archived and stored according to the standards set in Appendix H.

3.8 The Provider is responsible for maintaining data integration and communication between the Provider's system and the City's designated systems:

3.8.1 For the purposes of parking occupancy collection, the Provider is responsible for the successful transfer of parking occupancy data between the Provider and the City's designated Automatic Data Collection system as shown in Appendix D

3.8.2 For the purposes of the Police Department, the Provider is responsible for the successful transfer of citation, scofflaw and stolen vehicle information between the Provider and the City's citation, scofflaw and stolen vehicle databases as shown in Appendix D

#### **4 REPORT REQUIREMENTS**

##### **4.1 DISASTER RECOVERY PLAN AND SYSTEM RECOVERY**

4.1.1 Disaster Recovery/Backup Plan. It is the responsibility of the Provider to take every precaution to ensure that all systems, files, data, equipment, communications, and facilities are reliable. In the event that a natural disaster or some other unanticipated event does disrupt the system, the Provider must have a detailed, City-approved recovery plan in place, tested, and ready to be implemented for all key facilities so that services are restored quickly and in accordance with City performance standards.

#### 4.2 AUDITS, RECORDS TO BE MAINTAINED, ACCESS TO RECORDS

4.2.1 The Provider shall maintain account books, records, documents and other evidence directly pertinent to performance and billing of the work under the Contract, in accordance with generally accepted accounting practices. The Provider shall also maintain the financial information and data used by the Provider in the preparation or support of cost estimates to the City. The City, or its duly authorized representative, shall have access to such account books, records, documents, and other evidence, for the purpose of inspection, audit, and copying. The Provider shall provide proper facilities for such access. The Provider shall not charge the City for time spent assisting the City in reviewing said documents.

4.2.2 Audits conducted pursuant to this provision shall be in accordance with generally accepted auditing standards. The Provider agrees to provide full access to the City all information, reports, and records pursuant to this section. Where the audit concerns the Provider, the City's representative shall afford the Provider an opportunity for an audit exit conference and an opportunity to comment on the pertinent portions of the draft audit report. The final audit report shall include the written comments, if any, of the Provider.

4.2.3 The Provider shall maintain copies of the complete records of the execution of the Contract, including, but not limited to documents, as necessary to assist in the defense of any legal action claiming liability or neglect of duty which may involve the City. The City shall also have access to these records. These records shall be maintained for a period of not less than three years after the earliest date which the applicable statutes may establish for the release of potential liability for the services rendered or performed under the Contract.

4.2.4 Accounting records as above shall be maintained and made available during performance of the work under the Contract for three years from date the Contract ends. In addition, those records which relate to any appeal, contract, litigation, or the settlement of claims arising out of such performance or cost, or items to which

an audit exception has been taken, shall be maintained and made available until three years after the date of resolution of such appeals, litigation, claims, or exception.

**5 INSTALLATION/INSPECTION SHIPPING**

5.1 Provider shall be responsible for all shipping and delivery costs associated with original order. Future orders shall be FOB Destination – Prepay and Add Shipping

5.2 Provider shall deliver new, fully-tested equipment, at mutually agreed upon time(s) and date(s) under the supervision of the City.

**6 CITY'S RESPONSIBILITIES**

6.1 City staff, in conjunction with Provider's staff, shall inspect LPR equipment following installation to ensure proper installation and operation.

6.2 City shall evidence its acceptance of the equipment under the Agreement by delivery to the Provider of an Equipment Acceptance Certificate, similar to Appendix H of this Agreement, with respect thereto.

END OF APPENDIX B

APPENDIX C  
PAYMENT TERMS

This Appendix C is attached to and incorporated by reference with the Contract made on May 1, 2015 between the CITY OF BERKELEY ("City") and Portable Computer Systems, Inc. dba PCS Mobile, ("Provider"), providing for the licensing and services related to the License Plate Recognition Equipment and Software.

1 TOTAL CONTRACT PRICE:

Contract Price for the furnishing of all Licenses, Services and Equipment shall not exceed \$450,000. For the convenience of the parties, the Contract price includes the following expenses as noted in the price chart below:

PROPOSED COST ELEMENTS - SUMMARY	
Cost Element	Price
Mobile LPR Equipment and Install - Overtime Kit - 5 or more systems	\$ 189,260.00
Mobile Computing - Complete Kit	\$ 30,875.00
Spare Parts	\$ 19,235.00
Cellular Connection Costs (Shown as Annual Cost)	\$ 4,710.00
Miscellaneous On-call Services and Equipment	\$ 69,670.00

Costs Options - Extended Warranty and Mobile Assurance - Overtime Kit (Pricing if Purchase Five (5) or More Systems)

Item Number	Item	Item Description	Quantity	Unit Price	Extended Price
Extended Warranty and SMA Options					
	<b>SMA for Five Years</b>				
SMA-BASE-5Y		SMA Base Package = 5 years; this item replaces SMA-BASE-1Y if purchased at time of sale ** Replaces SMA-BASE-1Y if Chosen	1	\$ 1,200.00	\$ 1,200.00
	<b>Extended Warranty</b>				
AU-K-OXX-EWRR-P5		Extended Warranty for AU-K-OXX kit with Return and Repair coverage - Total warranty coverage of 5 Years when prepaid at time of system purchase (one year included in the selling price and four (4) additional years). This includes coverage of AutoVu vehicle hardware, Patroller software upgrades and Bing license renewal. Does not cover in-vehicle PC. **Option vs AU-K-OXX-EWRR-1Y purchased annually through Year 5	5	\$ 14,840.00	\$ 74,200.00
Subtotal					\$ 75,400.00
<b>Extended Warranty and SMA for total of Five (5) years of coverage</b>					<b>\$ 75,400.00</b>

Support - Mobile Assurance (annual Cost)				
MOB-MAMBaseCamp	Mobile Assurance® Mobility BaseCamp	Any service or support that requires a PCS Mobile Mobility Specialist to work with the customer via Phone, Email, Remote, and/or at the PCS Mobile Shop to resolve issues involving the AutoVu LPR solution in the vehicle.	5	\$ 100.00 \$ 500.00
MOB-SUPPORT	Mobile Assurance® BaseCamp Server	Any service or support that requires a PCS Mobile IT Specialist to work with the customer via Phone, Email, Remote, and/or at the PCS Mobile Shop to resolve issues involving the AutoVu LPR Software (i.e. Security Center or Patroller) on the server.	1	\$ 1,500.00 \$ 1,500.00
<b>Subtotal</b>				<b>\$ 2,000.00</b>
<b>Annual cost for Remote Support of Five (5) AutoVu Systems</b>				<b>\$ 2,000.00</b>

Support - Mobile Assurance Options (Per Incident Costs)				
MOB-MAPM	Preventative Maintenance	Optional Preventative Maintenance to include with any package. This visit includes checking and re-seating all connections, mounting hardware, testing and adjusting of hardware and software. (This cost will be incurred when instructed by City of Berkeley of needed service and at their sole discretion)	5	\$ 200.00 \$ 1,000.00
Travel_Zone_4	Travel Cost	Travel Cost per trip for Preventative Maintenance or On-Site Support	1	\$ 1,400.00 \$ 1,400.00
<b>Subtotal</b>				<b>\$ 2,400.00</b>
<b>Preventative Maintenance Costs for five (5) Units - Per Incident cost</b>				<b>\$ 2,400.00</b>



<b>Costs Options - Hosting and Custom Development</b>					
Item Number	Item	Item Description	Quantity	Unit Price	Extended Price
<b>Hosting Options</b>					
GSC-Av-MS-1Y	<b>Storage Server</b>	GSC AutoVu Managed Service for one (1) year. Max ten (10) Patroller connections included. No fixed camera connection supported. Max five (5) concurrent Security Desk connections. Limited functionalities (please refer to product description)	5	\$ 3,540.00	\$ 17,700.00
<b>Hosting Configuration</b>					
PS-AV-AMS-250-NA		Permit zone configuration services for AutoVu Mobile University or City with or without Wheel imaging Package (ex: Zone editor, mapping, custom enforcement rules). Maximum of 250 permit zones will be configured. (For "Autovu Managed Services" Deployment only)	1	\$ 1,250.00	\$ 1,250.00
<b>Services for Hosting</b>					
<b>Custom Development for Occupancy Functionality</b>					
PS-C-DEVELOP-NA	<b>Custom Development Services</b>	**Custom development of software for Occupancy functionality. This is an hourly cost for Genetec's Engineering Services. Time sheets will be provided for all of this work.	240	\$ 156.25	\$ 37,500.00
<b>Subtotal</b>					<b>\$ 56,450.00</b>
<b>Options and Services Cost Total</b>					<b>\$ 56,450.00</b>

\*\* Currently we provide a GPS coordinate for every read we export. What is proposed is we will include a BlockFace with every export. The Blockface will also be converted, using an excel spreadsheet from Berkeley, to the existing nomenclature used by Berkeley.  
 In essence we will be reporting the read data , and next to every read we will attach the block face. Xerox will need to convert that into a % of occupancy and possibly turnover.

**2 INVOICES**

Invoices shall contain itemized charges reflecting agreed upon unit prices or hourly billable rates as shown in this agreement with proper supporting documents.

**3 TIMING OF PAYMENTS**

**3.1 Payments Due Upon Delivery of Services.** City and Provider agree that any undisputed costs shown above shall be paid by the City upon completion of the service and acceptance by the City and within thirty (30) days of receipt of properly supported invoices from Provider.

Payment of any invoice shall not be deemed a waiver of any dispute.

City agrees that it shall promptly notify Provider in writing of any dispute with an invoice.

END OF APPENDIX C

**APPENDIX D****SPECIFICATIONS****LICENSE PLATE RECOGNITION EQUIPMENT AND SOFTWARE SYSTEM**

This document is intended for the Provider of the Functional LPR system that can be used for both occupancy detection and enforcement.

The system being specified here will be used by the City to capture vehicle occupancy in both demarcated and non-demarcated areas in the City. The occupancy data will be sent to the City's Automatic Data Collection system being developed by Xerox. The format of the data and the mechanism for data transfer shall be defined by Xerox.

In addition, the LPR system will integrate with City's existing systems e.g PPEO Handheld (Xerox), to provide time limit and illegal parking enforcement. The Provider shall work with the Providers of City's existing systems for the integration. The following sections and diagram describe the overall Automated Data Collection and Enforcement System solution.

**1. In-vehicle System**

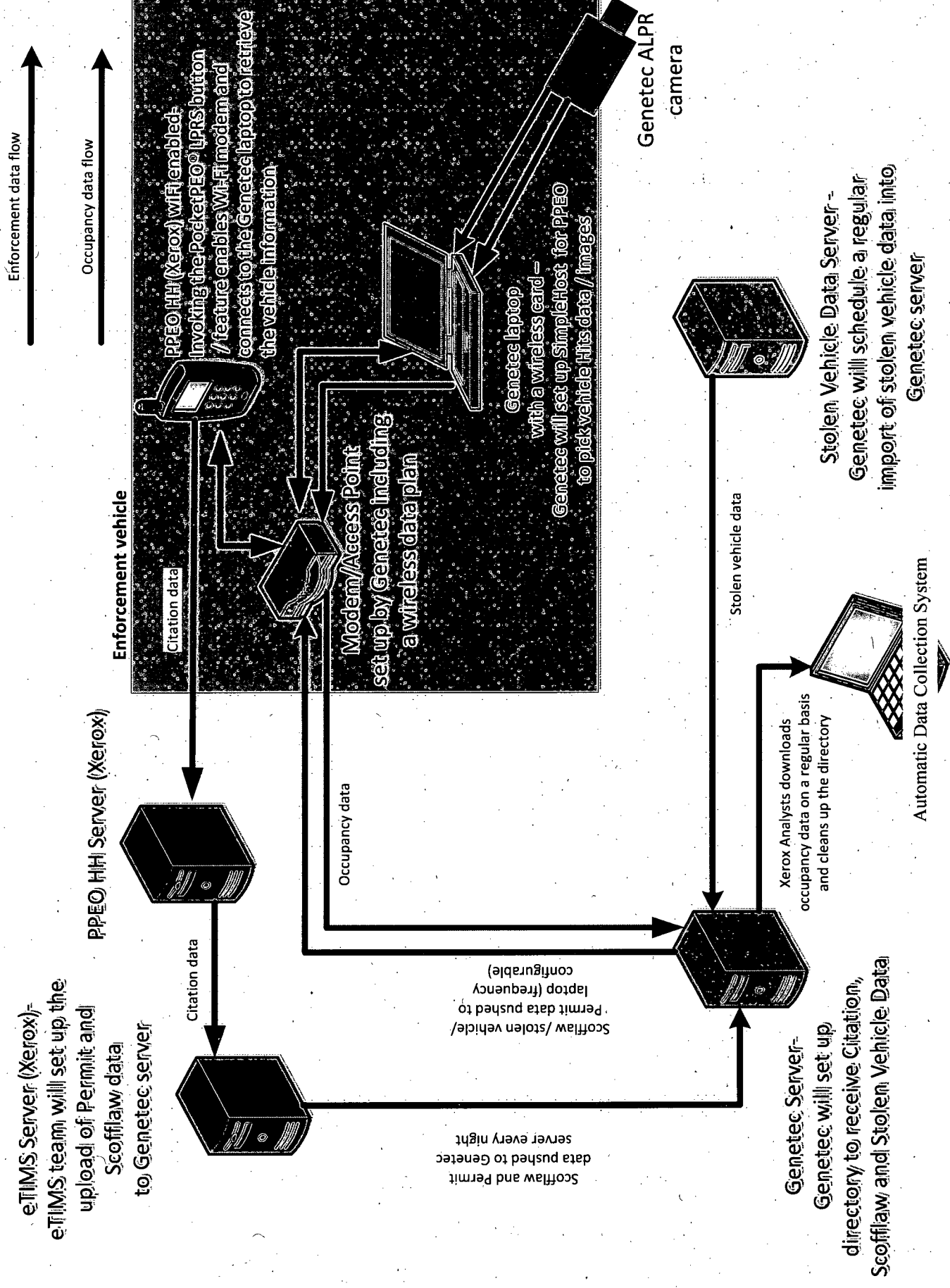
- a. ALPR system: The ALPR cameras including the license plate and wheel image cameras will capture and provide images to the in-vehicle Genetec laptop which will run the Security Desk, Patroller. Provider shall provide and install the ALPR cameras, laptop and other associated hardware/software
- b. Modem/Access point: Provider shall provide a modem/access point for wireless communication between Genetec laptop and PPEO handheld and for cellular wireless communications with the Genetec backend server. Provider shall also provide the monthly data plan with sufficient bandwidth required for real-time transfer of data from the in-vehicle laptop to the backend server.
- c. Provider shall coordinate with Xerox to set up the data transfer of vehicle "hits" data between the laptop and PPEO handheld.

**2. Backend system**

- a. Provider shall provide hosting for goBerkeley Automated Data Collection and Enforcement System. This server may be hosted by Genetec. Provider shall coordinate with Xerox to set up directories in the host server to receive residential permits and Scofflaw data from Xerox on a mutually agreed upon and City-configurable schedule.
- b. Provider shall configure the host server to receive the latest California Stolen Vehicles data from the CA Department of Justice Stolen Vehicle System (SVS) on a mutually agreed upon and City-configurable schedule.

- c. Provider shall configure the host server to push the latest residential permit, Scofflaw and Stolen vehicle data to the in-vehicle Genetec laptop on a mutually agreed upon and City-configurable schedule.
- d. Vendor shall configure the host server and in-vehicle laptop to transfer the vehicle occupancy data from the laptop to the server in real-time
- e. Vendor shall make available to Xerox the following information for occupancy:
  - i. Occupancy data by block face
  - ii. Occupancy data for each vehicle including high precision GPS coordinates (which according to Genetec will be available in the upcoming release of their new software)

Vendor shall provide access to Xerox for a regular download the occupancy data. Xerox will download the data from Genetec server.



eTIMS Server (Xerox) - eTIMS team will set up the upload of Permit and Scofflaw data to Genetec server

Scofflaw and Permit data pushed to Genetec server every night

Scofflaw / stolen vehicle/ Permit data pushed to laptop (frequency configurable)

Xerox Analysts downloads occupancy data on a regular basis and cleans up the directory

Automatic Data Collection System

Stolen Vehicle Data Server - Genetec will schedule a regular import of stolen vehicle data into Genetec server

Overall Description

The LPR system being specified here includes the hardware that will be deployed in the field and its associated backend system including hardware and software. It also includes the user interfaces that will be available to City users for monitoring the system.

System Perspective

The LPR system will be used in conjunction with the following systems/data sources:

- a) For Occupancy
  - System being developed by Xerox
    - Occupancy reporting data hub
    - City web site displaying parking occupancy statistics
  
- b) For Enforcement
  - Existing systems
    - Electronic handheld ticket writer software – currently PocketPEO® (Xerox)
    - Citation database – currently eTIMS® (Xerox) through PocketPEO handheld device
    - Law Enforcement Records Management System (LERMS)
    - Residential Parking Permit database – currently eTIMS® (Xerox)

Specifications

The LPR system must meet the following specifications:

Spec #	Specifications
1	The system shall detect the presence of a parallel parked vehicle in situations where parked vehicle bumpers are at least 12 inches apart.
2	The system shall be able to detect the presence of a stationary angle parked vehicle- defined as a stationary vehicle (angled between 45 and 90 degrees to the curb)

Spec #	Specifications
3	The system shall detect the presence of a parked vehicle, notwithstanding changes in illumination (shadows, sunlight, glare, day/night lighting transition)
4	The system shall detect a vehicle, the length of the vehicle notwithstanding ("Smart" Cars to tractor-trailer trucks, bicycles are NOT defined as vehicles in these requirements). Two and three wheeled vehicles are not included
5	The system shall detect vehicles simultaneously on both sides of the street
6	The system shall report the block face (per City's block face ID) where the detected vehicle is located
7	The system shall have a unique identifier for each vehicle (such as license plate, make, model, color or other unique data points) if detected as a parked vehicle
8	The system shall incorporate existing enforcement beat areas in each record
9	The system shall generate statistical reports by enforcement beat areas
10	The system shall integrate with current parking regulations information (eTIMS, PocketPEO) to automatically detect a parking time limit violation
11	The system shall incorporate multiple time limit zones on the same enforcement run.
12	The system shall integrate with current Residential Permit Parking (RPP) regulations to determine a permit zone violation; and a parking time limit violation within an RPP zone

Spec #	Specifications
13	The system shall display recorded data to the Parking Enforcement Officer on the LPR system laptop.
14	Report violation "alarms" that result from integration of recorded data with parking regulations to the Parking Enforcement Officer's handheld Computer in real-time. Violation alarms are desired for:
15	<ul style="list-style-type: none"> <li>• Violation of time limits in the City's 30 minute, 2 hr, 3hr and 8 hr time limit zones</li> </ul>
16	<ul style="list-style-type: none"> <li>• Violation of time limits and/or non-permit parking in the City's Residential Permit Parking zones</li> </ul>
17	The system shall allow PEO ability to override an alarm and enter an "exception" note or report. Overridden alarms will be tracked by time, day and PEO. Overridden data shall be a permanent record and cannot be modified or edited.
18	The system shall have a list of pre-defined common exceptions and allow entry of freeform comment
19	The system shall generate daily, weekly, monthly and annual statistical reports detailing but not limited to:
19.1	Total number of vehicle license plate reads
19.2	Total number of parking violations issued as a result of read vehicle license plate data. The report shall separate data for each Berkeley Municipal Code (BMC).
19.3	Total of parking violations not issued
19.4	Individual PEO enforcement activity and performance



Spec #	Specifications
20	The system shall ask the officer to login using unique security PIN and badge number
21	The detection system shall be mountable with temporary mounts on the following types of vehicles: (a) GO-4 (b) Sedan (c) SUV
22	The system shall record and store the state and number of a license plate with (n-2) 98% accuracy
23	The vendor shall provide ample processing power with the ability to dynamically scale CPU resources as needed for up to 25,000 spaces Citywide
24	The vendor shall provide disk space that is in accordance with the specifications listed in this document.
25	The system shall be scalable such that when additional resources such as processing power, memory allocation, or disk space are needed; the system will dynamically scale accordingly to handle data collection and enforcement of up to 25,000 spaces Citywide.
26	The vendor shall provide the appropriate bandwidth to meet or exceed the desired level of service to handle data collection and enforcement of up to 25,000 spaces Citywide.
27	The system shall accurately detect the presence of a parked vehicle at least 90% of the time
28	The system shall report accurate GPS coordinates at the time of vehicle detection at least 90% of the time

Spec #	Specifications
29	The system shall accurately report the block face where the vehicle is physically located at least 90% of the time
30	The system shall have a uniquely identify each vehicle (such as license plate, make, model, color or other unique data points)at least 98% of the time
31	All data shall be in real-time and actively available on PEO handheld on site at least 98% of the time
32	The vendor systems shall provide interfaces which support TCP/IP communications. Data exchange between systems shall be implemented via XML structured data over Web Services.
33	System to system communications shall be secured using SSL or IPsec.
34	The vendors shall work with Xerox during the requirements & design phases of the project to define and document data exchange file formats via interface control documents and XML XSD definitions.
35	The system shall record and store the date, day and time of the detection of a parked vehicle in the format defined for the Xerox-built Automatic Data Collection System
36	The system shall integrate with the Pilot's parking regulation and capacity database. At a minimum, the parking regulation and capacity database will list the number of legal parking spaces per block face with a unique block face ID

Spec #	Specifications
37	<p>The system shall provide data output that is compatible with the latest versions Microsoft SQL. As the new versions of Microsoft SQL become available, the provider will ensure compatibility. The proposed system should provide a way to store custom data elements and to enforce validation and business rules for that data. The system should further support the ability to include that data in reports and dashboards.</p>
38	<p>The system shall provide a data output that is compatible with ESRI data models.</p>
39	<p>The system shall keep the captured data (license plate information) secure. Adequate information security shall be applied to protect all data collected and stored to meet or exceed the standards listed in Appendix H. Systems through which data is passed or is stored shall be protected from unauthorized access from both internal and external sources.</p>
40	<p>The system shall have the capability to specify a separate user-configurable retention period on read and hit data. The retention settings shall result in all read/hit data captured before the specified period to be automatically purged without user intervention.</p>
41	<p>The vendor shall host supporting networks and systems outside of the City of Berkeley network.</p>
42	<p>The system shall provide a system with high availability and configured according to industry standard 99.999% of uptime or less than five (5) minutes of unscheduled downtime per year.</p>

Spec #	Specifications
43	The vendor shall provide adequate disaster recovery and take routine backups of the system with a four (4) hour Recovery Point Objective (RPO) and an eight (8) hour Recovery Time Objective (RTO).
44	The vendor shall provide security in accordance with industry standard SSAE 16 Type II for hosted solutions. Provider will protect system with the appropriate industry standard security provisions including firewall protection, AES 256 bit data encryption, antivirus protection, logging access of data and manipulation of data.
45	The vendor shall provide means to authenticate City personnel to access the equipment/service management system. The solution must allow for future integration in Active Directory when the system is hosted in the City
46	Provide a way to log different activities including, but not limited to, user authentication, file modification, user activity. Additionally, the system must provide a way to turn logging up such that debugging events may be achieved.
47	The vendor shall use virtualization technology that is compatible with VMware when the system is hosted in the City
48	The vendor shall provide City staff access to the system to perform any data manipulation that may be required. Ideally, this will be administered in a web based platform.

Spec #	Specifications
49	Provide an overall architecture that is in line with industry best practices. The design should use open standards protocols.
50	The vendor shall provide maintenance of the system such that service packs and patches are applied in a timely fashion. The provider is responsible for the health of the Operating System and Core applications.
51	The vendor shall adhere to UML documentation standards for workflow improvement and technology implementation projects and provide the proposed process flow and high level technical specifications for interface assumptions/requirements, required 3rd party components/services, and data exchange mechanisms.

END OF APPENDIX D

**APPENDIX E  
DETAILED TRAINING OUTLINE**

Portable Computer Systems, Inc dba PCS Mobile (“Provider”) shall provide the City with ongoing training to familiarize City staff with the mLPR units and the system. System training may be conducted by webinar or other remote educational methods; technical training must be conducted in person, no more than twice annually, not to exceed 10 business days annually. Additional training may be arranged as needed at a cost to the City.

The following training will be provided:

**1 Technical Training: (4 hour training sessions)**

The Provider shall provide City staff with in-depth, technical training on the functionality of the mLPR units. Training will be conducted in person, on an as needed basis no more than twice annually. Training dates will be scheduled, by mutual agreement, at least thirty days prior to the actual day. Technical training shall be divided into two sections: physical maintenance of the mLPR unit and virtual maintenance of the mLPR unit.

1.1 Physical Maintenance: At the conclusion of physical maintenance training, City staff will be able to maintain the hardware of the mLPR unit for day-to-day operation.

1.2 Virtual Maintenance: At the conclusion of virtual maintenance training, City staff will be able to operate system diagnostics and work with remote access staff to maintain the software that operates the mLPR units and interfaces with the City’s Automatic Data Collection System and enforcement systems.

1.3 Manual: Provider shall provide the City with a detailed training manual, discussing the above-mentioned areas of training.

END OF APPENDIX E

APPENDIX F

**LIMITED AND EXTENDED WARRANTIES (5-YEAR) SERVICE CONTRACT AND SOFTWARE MAINTENANCE & SUPPORT AGREEMENT**

- I. Portable Computer Systems, Inc. dba PCS Mobile shall provide the City with warranties and software maintenance services for the 5 year term of this contract. The terms of these warranties and software maintenance agreements are shown in the attached document titled: Warranty Levels and Software Maintenance Agreements, Version 5.
- II. **Charged-For-Enhancements.** From time to time, at Provider's sole discretion, Provider will make available to City Charged-for-Enhancements to the Software that City may license from Provider upon payment of the license fee established by Provider.
- III. **Software Functionality Enhancement Requests (Customizations).** If software functionality as outlined on the system documentation does not meet City's requirements, City may contract Provider to provided system functionality enhancements (customizations).

Provider will evaluate customization requests and provide City with a written change order that includes a scope of work and cost estimate prior to the development of customization specifications. Upon the City's written approval of the change order, Provider will prepare detailed customization specification for City's review and written approval prior to development.

The City must notify the Provider of customization functionality deficiencies (if customization does not function as outlined in approved specifications) within 60 days of customization delivery. Provider will correct all customization functionality deficiencies at no charge if notified within 60 days of delivery.

At Provider's discretion customer customizations may be added to the software's standard feature set and provided to Provider's other customers.
- IV. **On-Site Support.** Provider, will provide City On-Site Support as needed, as PCS MOBILE / GENETEC based on the terms and unit rates described in Appendix B, at the request of the City.
- V. **Network Hardware & Software Support.** Support & Maintenance services do not include: network support, monitoring, backup, installation or warranty on or of City's

network hardware or software.

**VI. Obligations of City.**

- A. *City Contact.* City shall notify Provider of City's designee. To the maximum extent practicable, City's communications with Provider will be through the City's designee(s).
- B. *Facility and Personnel Access.* City agrees to grant Provider access to City's facilities and personnel concerned with the mLPR operation to enable Provider to provide services.

END OF APPENDIX F



Appendix G

# Warranty Levels & Software Maintenance Agreements

Version 5

Innovative Solutions

**Genetec**

# Table of Contents

<b>1</b>	<b>Overview</b>	<b>5</b>
<b>2</b>	<b>Genetec's Standard Warranty Levels</b>	<b>6</b>
<b>2.1</b>	<b>Standard Software Warranty</b>	<b>6</b>
2.1.1	Standard Software Warranty Coverage	6
2.1.2	Products Covered by Standard Software Warranty	6
2.1.3	Summary of Standard Software Warranty	7
<b>2.2</b>	<b>Genetec's Standard Hardware Warranty</b>	<b>7</b>
2.2.1	Standard Hardware Warranty Coverage	7
2.2.2	Products Covered by Standard Hardware Warranty	8
2.2.3	Summary of Standard Hardware Warranty	8
2.2.4	Warranty on repairs and replacement parts	9
2.2.5	Exclusive Warranty Remedy	9
2.2.6	Warranty Exclusions	9
2.2.7	Relocation of AutoVu Mobile Systems	9
<b>3</b>	<b>Software Maintenance Agreements (SMA)</b>	<b>10</b>
<b>3.1</b>	<b>What is an SMA?</b>	<b>10</b>
<b>3.2</b>	<b>Products Covered by SMA</b>	<b>10</b>
<b>3.3</b>	<b>SMA</b>	<b>11</b>
<b>3.4</b>	<b>SMA Plus</b>	<b>12</b>
<b>3.5</b>	<b>SMA Value-Added Services Descriptions</b>	<b>13</b>
3.5.1	Priority Queuing	13
3.5.2	Technical Appointments	13
3.5.3	Remote System Assessment	13
3.5.4	On-Site System Assessment	13
3.5.5	Dedicated Support Engineer	13
a)	Shared Dedicated GTAC Support Engineer	14
b)	Dedicated GTAC Support Engineer	14
c)	Dedicated Onsite Support Engineer	14
3.5.6	Discount on Professional Services	14

<b>4</b>	<b>Genetec's Hardware Extended Warranties</b>	<b>15</b>
4.1	What is an Extended Warranty?	15
4.2	Summary of Extended Warranty with Return and Repair Coverage	15
4.3	Summary of Extended Warranty with Advanced Replacement Coverage	16
4.4	Exclusive Extended Warranty Remedy	16
4.5	Extended Warranty Exclusions	16
<b>5</b>	<b>Pricing &amp; Ordering</b>	<b>17</b>
5.1	<b>SMA</b> s	<b>17</b>
5.1.1	SMA Pricing Structure	17
5.1.2	SMA Multi-Year Discount	17
5.1.3	Multi System/Site SMA	17
5.1.4	SMA for License Add-ons	18
5.1.5	SMA Renewals	18
5.1.6	SMA Ordering Information	18
5.1.7	SMA Quoting Examples	19
a)	Example 1: Unified Video/ACS SC5 System	19
b)	Example 2: Multiple Systems with a Single SMA	19
c)	Example 3: Single Year SMA Add-on	20
d)	Example 4 : Multi-year SMA Add-on	20
5.2	<b>Hardware Extended Warranties</b>	<b>21</b>
5.2.1	Hardware Extended Warranty Availability	21
5.2.2	Hardware Extended Warranty Multi-Year Discount	21
5.2.3	Hardware Warranty Renewals	21
5.2.4	Hardware Extended Warranty Ordering Information	21
5.3	<b>"À la carte" upgrades and GTAC support</b>	<b>22</b>
5.3.1	Software upgrade – Major Release	22
5.3.2	Software upgrade – Minor Release	22
5.3.3	GTAC Support	22
5.3.4	On-Site Technical Support	22
5.3.5	Technical Appointments	23
<b>6</b>	<b>The Genetec Technical Assistance Center</b>	<b>23</b>
6.1	<b>Contacting the GTAC</b>	<b>23</b>

6.1.1	Via the Genetec Technical Assistance Portal (GTAP)	23
6.1.2	Via Phone	23
<b>6.2</b>	<b>Escalation Process</b>	<b>23</b>
<b>6.3</b>	<b>Support Case Life-cycle</b>	<b>24</b>
<b>7</b>	<b>GTAC Service Levels</b>	<b>25</b>
<b>7.1</b>	<b>Support Case Severity Levels</b>	<b>25</b>
7.1.1	Description of Severity Levels	25
7.1.2	Severity Level Examples	25
<b>7.2</b>	<b>Response Times</b>	<b>28</b>
7.2.1	First Response	28
7.2.2	Status Updates	28
7.2.3	Three Strike Rule - Follow up	29
<b>7.3</b>	<b>Resource Commitment</b>	<b>29</b>
<b>8</b>	<b>The Genetec Technical Assistance Portal</b>	<b>30</b>
<b>8.1</b>	<b>Accessing the GTAP</b>	<b>30</b>
<b>8.2</b>	<b>Available Resources</b>	<b>31</b>
8.2.1	System Management (Licenses)	31
8.2.2	GTAC Case Management	31
8.2.3	Documentation and Knowledge Base	31
8.2.4	Video and Webinars	31
8.2.5	Community Forums	32
8.2.6	Arrange for Technical Appointments	32
8.2.7	Supported Device Tool	32
8.2.8	Known Issues	32
8.2.9	GTAC Monthly Minute	32
<b>9</b>	<b>Appendix A – Software Warranty Lengths</b>	<b>33</b>
<b>10</b>	<b>Appendix B – Hardware Warranty Lengths</b>	<b>34</b>

# 1 Overview

The following document describes the warranty levels, Software Maintenance Agreements (SMAs) and Hardware Extended Warranties offered by Genetec for products developed, manufactured and sold by Genetec.

## 2 Genetec's Standard Warranty Levels

### 2.1 Standard Software Warranty

#### 2.1.1 Standard Software Warranty Coverage

Genetec warrants that its software products will perform in all material respects in accordance with the accompanying user manual, and the media on which the Software Product resides will be free from defects in materials and workmanship under normal use.

The Standard Warranty covers any Technical Assistance required from Genetec as a result of a Software defect.

#### 2.1.2 Products Covered by Standard Software Warranty

All packaged software products developed by Genetec, including but not limited to, Security Center Security Center Mobile, Omnicast, Synergis and AutoVu Patroller.

All custom software applications developed by Genetec using one of Genetec's SDK.

### 2.1.3 Summary of Standard Software Warranty

GTAC Support	
GTAC Hours	GTAC business hours <sup>1</sup>
Support Cases	Optional <sup>2</sup>
On-Site Support	Optional
Priority Queuing	n/a
GTAP Access	
System Management	Included
Case Management	Included
Knowledge Base	Included
Computer Based Training Courses	Included
User Forums	Included
Monthly Minute Newsletter	Included
Software Subscription Services	
Service Releases and Hot Fixes	Included
Minor Release Upgrades	n/a
Major Release Upgrades	n/a
Value Added Services	
Technical Appointments	Included
Remote System Assessment	n/a
On-site System Assessment	n/a
Dedicated GTAC Support Engineer	n/a
Dedicated Onsite Support Engineer	n/a
Discount on Services (including training)	n/a
Warranty Period	
Length of SMA	According to product <sup>3</sup>
Warranty Start Date	30 days after license issuance

<sup>1</sup>: GTAC business hours are from Monday through Friday, 8am to 8pm Eastern Time. The GTAC is closed on Canadian statutory holidays.

<sup>2</sup>: Support cases are available for purchase on systems without SMA coverage with the exception of license related issues and product defects.

<sup>3</sup>: Product standard warranty lengths and maximum extended warranty lengths can be found in Appendix A.

## 2.2 Genetec's Standard Hardware Warranty

### 2.2.1 Standard Hardware Warranty Coverage

Genetec warrants each product it manufactures to be free from defects in materials and assembly in the course of normal use and service, and provides technical assistance related to these defects.

Genetec Hardware Warranties cover both the product Hardware and Software running on the product, with the exception of appliances running one of Genetec's software products (ex: SV-16) in which case the Software Warranty takes precedence over the hardware warranty for software related issues.

The Genetec Standard Hardware Warranty does not cover labor to send a Genetec engineer on-site to evaluate a system problem and/or determine if there is a warranty issue or not and/or replace a defective product.

**2.2.2 Products Covered by Standard Hardware Warranty**

All hardware products manufactured or resold by Genetec, including but not limited to, AutoVu Sharp, AutoVu SharpX, HID VertX, SV-16 are covered by the Standard Warranty.

**2.2.3 Summary of Standard Hardware Warranty**

<b>GTAC Support</b>	
<b>GTAC Hours</b>	GTAC business hours <sup>1</sup>
<b>Support Cases</b>	Unlimited
<b>On-Site Support</b>	Optional
<b>Priority Queuing</b>	n/a
<b>In Warranty Repairs</b>	
<b>Product Return and Repair</b>	Included <sup>3,4,5</sup>
<b>Advanced Replacement of Defective Product</b>	Included within 90 days of purchase
<b>Unit Repair Turnaround time</b>	10 business days between receipt by Genetec and ship date to customer
<b>Functional Product Return</b>	Service charge for returned product with no defect found
<b>Product DOA (within 90 days of shipment)</b>	Free advanced replacement of a new product
<b>Product Software Updates/Upgrades</b>	
<b>Product Software Updates/Upgrades</b>	Included
<b>GTAP Access</b>	
<b>System Management</b>	Included
<b>Case Management</b>	Included
<b>Knowledge Base</b>	Included
<b>Computer Based Training Courses</b>	Included
<b>User Forums</b>	Included
<b>Monthly Minute Newsletter</b>	Included
<b>Warranty Period</b>	
<b>Length of Warranty</b>	According to product <sup>6</sup>
<b>Warranty Start Date</b>	On the day the product is delivered

<sup>1</sup> GTAC business hours are from Monday through Friday, 8am to 8pm Eastern Time. The GTAC is closed on Canadian statutory holidays.  
<sup>2</sup> Support cases are available for purchase on systems under Standard Warranty without Extended Hardware Warranty with the exception of product defect related issues  
<sup>3</sup> Additional charges may be applied if damage is a result of using the product in a way that it is not typically intended to be used.  
<sup>4</sup> Product may be replaced by a fully functional refurbished product.  
<sup>5</sup> Customer is responsible for all shipping charges to return the product back to Genetec, and Genetec will cover the shipping charges to send the product back to the customer.  
<sup>6</sup> Product standard warranty lengths and maximum extended warranty lengths can be found in Appendix B.



#### 2.2.4 Warranty on repairs and replacement parts

All Genetec products serviced by Genetec for repairs and replacements parts are warranted against defects in workmanship and materials for a period of 90 days, or the remainder of the original warranty, whichever is the longest.

#### 2.2.5 Exclusive Warranty Remedy

During the applicable warranty period and in the event that a product is determined by Genetec to be defective in materials or assembly, Genetec will at its sole discretion either credit the customer the price paid for the defective product, or repair the defective product without charge, or replace the defective product with a new or refurbished product, or replace the defective product with a different product with identical or better specifications.

#### 2.2.6 Warranty Exclusions

The following items are not covered by Genetec's Standard Hardware Warranty:

- Any equipment not furnished by Genetec
- A product which is used with non-supported ancillary equipment or software.
- Freight cost to return a product to Genetec.
- Defects or damage resulting from customer's improper testing, operation, installation, maintenance, modification, alteration, or adjustment.
- Defects or damage from misuse, accident or neglect.
- Defects or damage resulting from use of the product in other than its normal and customary manner.
- Defects or damage resulting from drilling holes, adding decals or other adhesives, or by painting the product.
- Defects or damage due to lightning or other electrical discharge.
- Product that is disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection and testing to verify any warranty claim.
- Modification or abuse of, or tampering with, the product.
- Normal wear and tear.

#### 2.2.7 Relocation of AutoVu Mobile Systems

Relocating a hard mounted AutoVu Mobile System from one vehicle to another will void the warranty on the cables. This does not apply to portable systems with magnetic mounts.

## 3 Software Maintenance Agreements (SMA)

### 3.1 What is an SMA?

An SMA provides customers with any new software releases, both minor and major updates, as well as unlimited access to Technical Support. The SMA protects the investment that is made in the solution by maintaining the systems up to date with the latest technological innovations developed by Genetec, by ensuring that the system operates and functions optimally and that the users leverage the system's full potential in order to generate maximum ROI of the solution.

### 3.2 Products Covered by SMA

All packaged software products developed by Genetec, including but not limited to, Security Center Security Center Mobile, Omnicast, Synergis and AutoVu Patroller.

All custom software applications developed by Genetec using one of Genetec's SDKs.

All software upgrades performed under the SMA continue to be covered by the SMA as long as it is in force.

## 3.3 SMA

GTAC Support	
GTAC Hours	GTAC business hours + customers business hours <sup>1</sup>
Support Cases	Unlimited
On-Site Support	Optional
Priority Queuing	Included <sup>3</sup>
GTAP Access	
System Management	Included
Case Management	Included
Knowledge Base	Included
Computer Based Training Courses	Included
User Forums	Included
Monthly Minute Newsletter	Included
Software Subscription Services	
Service Releases and Hot Fixes	Included
Minor Release Upgrades	Included
Major Release Upgrades	Included
Value Added Services	
Technical Appointments	Included
Remote System Assessment	Optional
On-site System Assessment	Optional
Dedicated GTAC Support Engineer	n/a
Dedicated Onsite Support Engineer	n/a
Discount on Services (including training)	5%
SMA Period	
Length of SMA	1-5 year terms
SMA Start Date	30 days after license issuance or on SMA anniversary date for a renewal

- <sup>1</sup> GTAC business hours are from Monday through Friday, 8am to 8pm Eastern Time. The GTAC is closed on Canadian statutory holidays.  
<sup>2</sup> Done via pager if outside GTAC standard support hours with the exception of Canadian statutory holidays when the GTAC is closed.  
<sup>3</sup> Customers with a valid SMA will get priority queuing over customers without an SMA when contacting the GTAC via phone.  
<sup>4</sup> Each SMA includes 4 hours of Technical Appointments per year.

## 3.4 SMA Plus

GTAC Support	
GTAC Hours	7x24 <sup>1</sup>
Support Cases	Unlimited
On-Site Support	Optional
Priority Queuing	Included <sup>2</sup>
GTAP Access	
System Management	Included
Case Management	Included
Knowledge Base	Included
Computer Based Training Courses	Included
User Forums	Included
Monthly Minute Newsletter	Included
Software Subscription Services	
Service Releases and Hot Fixes	Included
Minor Release Upgrades	Included
Major Release Upgrades	Included
Value Added Services	
Technical Appointments	Included <sup>3</sup>
Remote System Assessment	Included <sup>4</sup>
On-site System Assessment	Optional
Dedicated GTAC Support Engineer	Optional
Dedicated Onsite Support Engineer	Optional
Discount on Services (including training)	10%
SMA Period	
Length of SMA	1-5 year terms
SMA Start Date	30 days after license issuance or on SMA anniversary date for a renewal.

<sup>1</sup> Done via pager outside GTAC standard support hours.

<sup>2</sup> Customers with a valid SMA will get priority queuing over customers without an SMA when contacting the GTAC via phone.

<sup>3</sup> Each SMA Plus includes 8 hours of Technical Appointments per year.

<sup>4</sup> Each SMA Plus includes one Remote System Assessment per year.

**3.5 SMA Value-Added Services Descriptions**

**3.5.1 Priority Queuing**

Customers with a valid SMA will get priority in the queue over customers without an SMA when calling the GTAC. When multiple customers with valid SMAs are in the queue simultaneously, priority is given on a first come first served basis.

**3.5.2 Technical Appointments**

Customers with a valid SMA may schedule technical appointments with a Genetec Technical Support Engineer. Technical appointments may be used to discuss system design, plan a system upgrade, assist during a system upgrade or used for any other product-related technical work.

Technical appointments can be booked on the GTAP. Technical appointments must be scheduled during regular GTAC hours but are also available after hours, if needed, at an extra cost.

Each SMA type includes a predefined block of hours to be used each year for technical appointments as detailed in the table below. Additional hours may be purchased if needed.

Type of SMA	Included appointment hours	Maximum number of appointments
SMA	4 hours	2
SMA Plus	8 hours	4

**3.5.3 Remote System Assessment**

A GTAC engineer will remotely connect to the customer system and perform a standard technical system assessment and provide recommendations. A report will be sent out to the customer at the end of the remote system assessment. The Remote System Assessment is a complementary service offered to SMA Plus customers once per year. This service is also available for purchase to SMA customers.

In order to provide this service, customer must provide the GTAC with a valid remote connection to their site.

**3.5.4 On-Site System Assessment**

Receive a visit from a Genetec Field Engineer onsite. During this visit, the Field Engineer can do a technical assessment of the system, perform system maintenance, discuss system design or perform various other tasks. The length of the visit will be evaluated by Genetec based on the Scope of Work.

**3.5.5 Dedicated Support Engineer**

Customers will be assigned a Dedicated Support Engineer. This Engineer will act as the main point of contact for all support related issues and will be familiar with the system design and its intricacies.

There are three different options available for this service:

**a) Shared Dedicated GTAC Support Engineer**

The assigned Dedicated GTAC Support Engineer will be responsible to support several dedicated client accounts. Therefore, customers acquiring this service will essentially be sharing the Dedicated GTAC support engineer with up to 5 other customers.

Customers with a Shared Dedicated GTAC Support Engineer will be assigned a specific 1-800 number (for North American customers only) and email address. Outside of the GTAC's business hours, customers must go through the regular support queues in order to obtain immediate assistance.

**b) Dedicated GTAC Support Engineer**

The assigned Dedicated GTAC Support Engineer will be responsible to exclusively support a single customer.

Customers with a Dedicated GTAC Support Engineer will be assigned a specific 1-800 number (for North American customers only) and email address. Outside of the GTAC's business hours, customers must go through the regular support queues in order to obtain immediate assistance.

**c) Dedicated Onsite Support Engineer**

The Dedicated Onsite Support Engineer will reside at the customer's premises and provide proactive assistance, reactive support and system management.

The Dedicated Onsite Support Engineer is generally available during business hours on business days unless otherwise agreed upon.

**3.5.6 Discount on Professional Services**

Customers with a valid SMA will benefit from discounts on all Genetec professional services, including Technical Training as detailed in the table below.

Type of SMA	Discount on Services
SMA	5%
SMA Plus	10%

## 4 Genetec's Hardware Extended Warranties

### 4.1 What is an Extended Warranty?

An Extended Warranty provides the means to extend the standard warranty length of hardware products sold by Genetec and that are eligible for a warranty extension. (See Appendix B – Hardware Warranty Lengths)

### 4.2 Summary of Extended Warranty with Return and Repair Coverage

GTAC Support	
GTAC Hours	GTAC standard support hours <sup>1</sup>
Support Case Allowance	Unlimited
On-Site Support	Optional
Priority Queuing	n/a
In Warranty Repairs	
Product Return and Repair	Included <sup>2,3,4</sup>
Advanced Replacement of Defective Product	Included within 90 days of product purchase
Unit Repair Turnaround time	10 business days between receipt by Genetec and ship date to customer
Functional Product Return	Service charge for returned product with no defect found
Product Software Updates/Upgrades	
Product Software Updates/Upgrades	Included
GTAP Access	
System Management	Included
Case Management	Included
Knowledge Base	Included
Computer Based Training Courses	Included
User Forums	Included
Monthly Minute Newsletter	Included
Warranty Period	
Length of Extended Warranty	According to product <sup>5</sup>
Warranty Start Date	On the day the product is delivered

<sup>1</sup> GTAC standard support hours are from Monday through Friday, 8am to 8pm Eastern Time. The GTAC is closed on Canadian statutory holidays.

<sup>2</sup> Additional charges may be applied if damage is a result of using the product in a way that it is not typically intended to be used.

<sup>3</sup> Product may be replaced by a fully functional refurbished product.

<sup>4</sup> Customer is responsible for all shipping charges to return the product back to Genetec, and Genetec will cover the shipping charges to send the product back to the customer.

<sup>5</sup> Product standard warranty lengths and maximum extended warranty lengths can be found in Appendix B.

### 4.3 Summary of Extended Warranty with Advanced Replacement Coverage

GTAC Support	
GTAC Hours	GTAC standard support hours <sup>1</sup>
Support Case Allowance	Unlimited
On-Site Support	Optional
Priority Queuing	n/a
In Warranty Repairs	
Product Return and Repair	n/a
Advanced Replacement of Defective Product	Included <sup>2,3,4</sup>
Unit Repair Turnaround Time	Customer is responsible for replacing and returning the defective product to Genetec <sup>3</sup> within 30 days; otherwise the MSRP of product will be invoiced to the customer
Functional Product Return	Service charge for returned product with no defect found
Product Software Updates/Upgrades	
Product Software Updates/Upgrades	Included
GTAP Access	
System Management	Included
Case Management	Included
Knowledge Base	Included
Computer Based Training Courses	Included
User Forums	Included
Monthly Minute Newsletter	Included
Warranty Period	
Length of Extended Warranty	According to Product <sup>5</sup>
Warranty Start Date	On the day the product is delivered

<sup>1</sup> GTAC standard support hours are from Monday through Friday, 8am to 8pm Eastern Time. The GTAC is closed on Canadian statutory holidays.

<sup>2</sup> Additional charges may be applied if damage is a result of using the product in a way that it is not typically intended to be used.

<sup>3</sup> Product may be replaced by a fully functional refurbished product.

<sup>4</sup> Genetec is responsible for shipping charges for both sending the replacement product to the customer and returning the defective product back to Genetec.

<sup>5</sup> Product standard warranty lengths and maximum extended warranty lengths can be found in Appendix B.

### 4.4 Exclusive Extended Warranty Remedy

See Section 2.2.5: Exclusive Warranty Remedy

### 4.5 Extended Warranty Exclusions

See Section 2.2.6: Warranty Exclusions



## 5 Pricing & Ordering

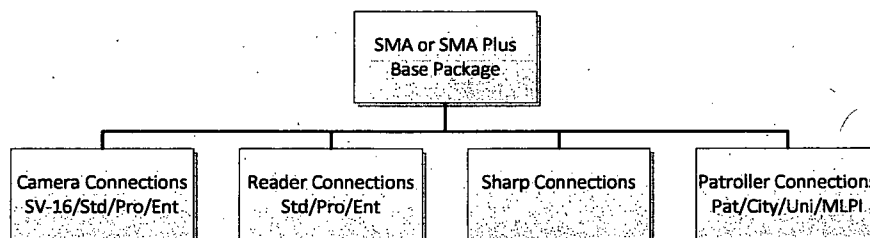
### 5.1 SMAs

#### 5.1.1 SMA Pricing Structure

SMAs are assembled in a similar fashion to Genetec software licenses, meaning that it's composed of a base package (for either an SMA or an SMA Plus) and a number of options depending on the system(s) covered by the SMA in question.

It is important to note that not all software license options have a corresponding SMA line item; in fact very few license options have that. If we take the example of Omnicast, only camera connection licenses are counted when pricing an SMA, all other license options/connections are SMA-free. It is therefore very simple to quickly assemble an SMA quote with just a few line items.

Since the difference between the SMA and the SMA Plus is taken into account in the SMA base package, all other line items that form the SMA are the same regardless what type of SMA has been selected.



#### 5.1.2 SMA Multi-Year Discount

Genetec offers multi-year SMA terms in the form of a 2-year, 3-year, 4-year or 5-year agreement. All SMA line items have their respective multi-year counterparts that are used for ordering a multi-year SMA.

Since these multi-year SMAs represent a long term commitment to Genetec, an additional discount is factored in all multi-year SMA line items. In order to benefit from this multi-year discount, the full amount for a multi-year SMA must be paid in full at the time of purchase or renewal.

#### 5.1.3 Multi System/Site SMA

An SMA can cover multiple System IDs, therefore an **end-user** with multiple system can consolidate all his systems under a single SMA for added simplicity. Since there's effectively only one SMA in this scenario, the end-user will only pay for the SMA base package once for the entire SMA and **NOT** once for every System ID covered by the SMA, therefore benefiting from a volume discount for placing all of his Genetec systems under a unique SMA.

It is important to note that a reseller **CANNOT** place multiple System IDs from multiple end-users under a single SMA.

#### 5.1.4 SMAs for License Add-ons

An SMA is mandatory for all add-ons done to an existing system that is currently under SMA. However, this applies only to software options for which Genetec charges an SMA for (Cameras, Readers, Sharps and Patrollers).

When adding a software license option that has a corresponding SMA line item, the SMA price for that add-on must be pro-rated to co-terminate with the SMA's anniversary date. This is accomplished by using a series of "1 day" SMA part numbers that are created solely to facilitate the pro-rating calculation.

In order to compute the price, simply take the appropriate SMA 1 day part number associated to the license option that is being added to the system, multiply that by the quantity of license options ordered and then multiply that again by the number of days remaining in the SMA term. Information on an SMA's anniversary date and remaining days in the agreement is readily accessible through the system management section of the GTAP.

#### 5.1.5 SMA Renewals

Renewal notices are automatically sent 90 days and 45 days prior to the anniversary date of the SMA, indicating that the SMA is about to expire. In the eventuality that the SMA is not renewed by the anniversary date, an additional notice is sent advising of the expiration of the SMA.

SMA coverage must be continuous. For example, if year two is skipped and an SMA is desired for year three, the cost of the SMA will be retroactive to include the year that was skipped, thus will cover both the second and third year.

All SMA renewals are priced according to the most recent price list in effect at the time of the renewal.

#### 5.1.6 SMA Ordering Information

SMAs must be purchased together with a new system sale or in conjunction with a system upgrade. If an SMA is purchased as an add-on to an existing system, it will be priced retroactively as if it was purchased at the same time as the system it will cover.

To order an SMA, the base package must be selected first for either an SMA or an SMA PLUS by using the following line items:

SMA-BASE-XX or SMA-PLUS-XX

Once the SMA base package has been selected, the other SMA line items are chosen based on the content of the licenses that the SMA covers. The format for all SMA part numbers follows the following standard:

SMA-0000-E-XX or SMA-0000-XX

Where:

**OOO:** License option reference: CAM (Camera Connection), RDR (Reader Connection), SHP (AutoVu Sharp Connection), PATR (AutoVu Patroller System), UNIV (AutoVu University System), CITY (AutoVu City System) and MLPI (AutoVu MLPI System)

**E:** Edition of the software if applicable: S (Standard), P (Pro), E (Enterprise)

**XX:** The term of the SMA: 1Y, 2Y, 3Y, 4Y, 5Y and 1D.

Complete SMA pricing information is found in the SMA price list.

**5.1.7 SMA Quoting Examples**

**a) Example 1: Unified Video/ACS SC5 System**

Customer purchases a unified Video/ACS SC5 system. He purchased the Enterprise version of Synergis with 50 Readers, the Pro version of Omnicast with 75 Camera, has 2 Sharp Cameras and requires a 3 year SMA.

The parts required to assemble this SMA would be as follows:

Part No	Description	Qty
SMA-BASE-3Y	SMA Base Package – 3 years	1
SMA-CAM-P-3Y	SMA for 1 Omnicast Pro Camera – 3 years	75
SMA-RDR-E-3Y	SMA for 1 Synergis Enterprise Reader – 3 years	50
SMA-SHP-3Y	SMA for 1 Sharp Camera – 3 years	2

**b) Example 2: Multiple Systems with a Single SMA**

Customer has an extensive multi-site deployment with federation, with both Video and ACS. Customer requires a 1 year agreement with round the clock access to Technical Support and has the following sites to deploy:

Site	Video	Access Control
Site A	Omnicast Enterprise 350 cams	Synergis Enterprise 40 readers
Site B	Omnicast Enterprise 120 cams	Synergis Enterprise 25 readers
Site C	Omnicast Pro 60 cams	Synergis Enterprise 10 readers
Site D	Omnicast Standard 15cams	Synergis Enterprise 5 readers
Site E	Omnicast Standard 15cams	Synergis Enterprise 5 readers

To summarize, the customer has 470 Omnicast Enterprise cameras, 60 Omnicast Pro cameras, 30 Omnicast Standard cameras and 85 Synergis Enterprise readers. The parts required to assemble this SMA would be as follows:

Part No	Description	Qty
SMA-PLUS-1Y	SMA Plus Base Package – 1 year	1
SMA-CAM-S-1Y	SMA for 1 Omnicast Standard Camera – 1 year	30
SMA-CAM-P-1Y	SMA for 1 Omnicast Pro Camera – 1 year	60
SMA-CAM-E-1Y	SMA for 1 Omnicast Enterprise Camera – 1 year	470
SMA-RDR-E-1Y	SMA for 1 Synergis Enterprise Reader – 1 year	85

**c) Example 3: Single Year SMA Add-on**

Customer has an existing unified Video/ACS SC5 system. He purchased the Enterprise version of Synergis with 50 Readers, the Pro version of Omnicast with 75 Camera, has 2 Sharp Cameras and has an SMA Plus that ends on October 12<sup>th</sup> 2012. (Information available on the GTAP)

Customer adds an extra building to his system with an additional 25 Omnicast Pro cameras and 12 Synergis Enterprise readers on July 16<sup>th</sup> 2012, which means 89 days are left on his SMA. (Information available on the GTAP)

Since the customer is adding 25 cameras and 12 readers, this means that we must compute 25 x 89 Omnicast Pro Camera 1 Day SMA parts and 12 x 89 Synergis Enterprise Reader 1 Day SMA parts as shown below:

Part No	Description	Qty
SMA-CAM-P-1D	SMA for 1 Omnicast Pro Camera – 1 day	2,225
SMA-RDR-E-1D	SMA for 1 Synergis Enterprise Reader – 1 day	1,068

**d) Example 4 : Multi-year SMA Add-on**

Customer has an existing unified Video/LPR SC5 system. The system is composed of 500 Omnicast Enterprise Cameras, 20 AutoVu Sharp Cameras, 5 AutoVu Patrollers and has an SMA that ends on March 14<sup>th</sup> 2014. (Information is available on the GTAP)

Customer expands his fleet of AutoVu Patrollers by adding 5 extra vehicles on September 4<sup>th</sup> 2012, which means there are 557 days left in the SMA. (Information available on the GTAP)

Since the customer is adding 5 patrollers, this means that we must compute 5 x 557 Patroller 1 Day SMA parts as shown below:

Part No	Description	Qty
SMA-PATR-1D	SMA for 1 AutoVu Patroller – 1 day	2,785

## 5.2 Hardware Extended Warranties

### 5.2.1 Hardware Extended Warranty Availability

Extended warranties are only available for certain hardware products and kits. In order to determine for which product line is eligible for an extended warranty, please refer to "Appendix B – Hardware Warranty Lengths".

### 5.2.2 Hardware Extended Warranty Multi-Year Discount

Genetec offers multi-year Extended Warranty terms in the form of a 2 year, 3 year, 4 year or 5 year agreement; however the maximum length of an extended warranty will vary depending on the product it is purchased for. (See Appendix B – Hardware Warranty Lengths) All Extended Warranty line items have their respective multi-year counterparts that are used for ordering a multi-year Extended Warranty.

Since these multi-year agreements represent a long term commitment to Genetec, an additional discount is factored in to all multi-year Extended Warranty line items. In order to benefit from this long term commitment discount, the full amount for a multi-year Extended Warranty must be paid in full at the time of purchase or renewal.

### 5.2.3 Hardware Warranty Renewals

Hardware Warranty renewal notices are automatically sent 90 days and 45 days prior to the anniversary date, indicating that the Warranty is about to expire. In the eventuality that the Warranty is not renewed by the anniversary date, an additional notice is sent advising of the expiration of the Warranty.

Hardware Extended Warranty coverage must be **continuous**. If the warranty is not extended/renewed prior to its expiry, it will not be extendable any more.

All Hardware Extended Warranty renewals are priced according to the most recent price list in effect at the time of the renewal.

### 5.2.4 Hardware Extended Warranty Ordering Information

Genetec's hardware extended warranty prices can be found in Genetec's price book. Different product codes have been created for each product as well as their respective list of available extended warranty options. Please use the following rule to build the product code associated to the warranty options you have selected for the product you are purchasing.

AU-K-KKK-EWLL-YY or AU-S-EWLL-YY

Where:

**KKK:** Type of AutoVu kit, according to the part number of the kit that you ordered, the warranty applies to.

**LL:** Level of Warranty: RR for Return & Repair, AS for Advanced Replacement and AP for Advanced Replacement with 7x24 support

**YY:** Term of the Warranty (Y for year and P for prepaid): Y1, Y2, Y3, Y4, Y5, P2, P3, P4 and P5

When purchasing an extended warranty on a kit, only serialized items are covered by the extended warranty. Other items such as cables and mounting hardware are only covered by the standard hardware warranty.

### 5.3 “À la carte” upgrades and GTAC support

#### 5.3.1 Software upgrade – Major Release

Customers without an SMA may upgrade to the latest major software release, provided that their current system is only 1 major release back. For example, you may upgrade from version 4.2 to 5.0, but you cannot upgrade from version 3.5 to 5.0.

The upgrade cost is 35% of total system price based on the latest software price list and comes with a limited 90 day warranty as detailed in *section 2.1*.

#### 5.3.2 Software upgrade – Minor Release

Customers without an SMA may upgrade to the latest minor software release provided that they are within the same major release. For example, you may upgrade from version 4.7 to 4.8, but you cannot upgrade from version 4.7 to 5.1.

The upgrade cost is 25% of total system price based on the latest software price list and comes with a limited 90 day warranty as detailed in *section 2.1*.

#### 5.3.3 GTAC Support

Customers without an SMA may contact the GTAC but must pay a flat fee in order to open a support case, with the exception of all license related issues. Pricing information on support cases can be found in the SMA price list.

If the product is still under warranty when the support case is opened and that the investigation reveals that the root cause of the incident is a product defect, the full amount of the purchased support case will be refunded.

#### 5.3.4 On-Site Technical Support

On-site Technical Support is available to all customers and subject to availability of the Genetec Field Engineering team. Pricing information on Genetec Field Services can be found in the Genetec Professional Services price list.

### 5.3.5 Technical Appointments

Customers with an SMA who have consumed all of their Technical Appointment hours or customers who do not have an SMA and that wish to purchase Technical Appointment hours may do so by purchasing a minimum block of 4 hours. Pricing information on Technical Appointment hours can be found in the Genetec SMA price list.

## 6 The Genetec Technical Assistance Center

### 6.1 Contacting the GTAC

#### 6.1.1 Via the Genetec Technical Assistance Portal (GTAP)

The GTAC can be contacted by opening a Support Case through the Case Management Section of the GTAP. All support cases whether opened or resolved, created through the GTAP or through other means can be consulted through the GTAP in order to get the latest status or to communicate with the GTAC Engineer assigned to the case.

GTAP URL: <http://gtap.genetec.com>

#### 6.1.2 Via Phone

The GTAC offers phone support from Monday to Friday 8am-8pm EST/EDT and is closed during Canadian Statuary Holidays. After-hour support is available to SMA and SMA Plus owners according to the terms stated in the agreement.

When calling the GTAC it is important to have the Genetec System ID and the SMA Contract number (if applicable) in order to speed up the entitlement process:

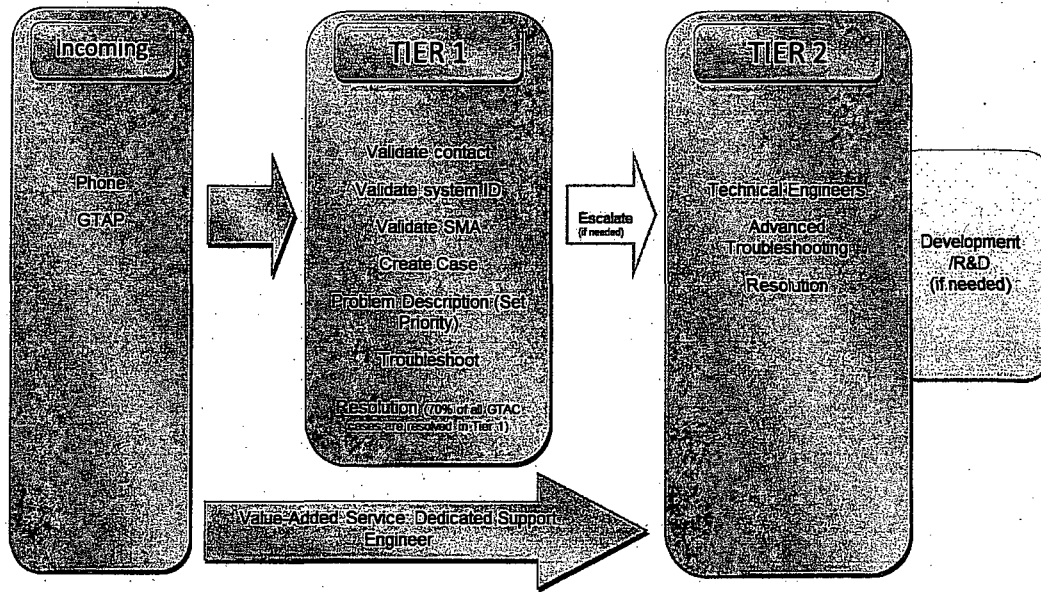
Direct Dial: 1-514-856-7100

Toll Free: 1-866-338-2988 (Canada & USA) | +800 01818200 (Europe)

### 6.2 Escalation Process

In the event a support case needs immediate attention of the GTAC's leadership team, there is a quick and simple way to ensure this will be done. Cases can be escalated via the GTAP's case management section. Clicking the "escalate" button will send a notification email to all members of the GTAC Leadership team regarding the urgency of the issue. We guarantee that the owner of the case will be contacted by a member of the GTAP leadership team within 1 business day.

### 6.3 Support Case Life-cycle





# 7 GTAC Service Levels

## 7.1 Support Case Severity Levels

### 7.1.1 Description of Severity Levels

Severity	Description
Critical	Product is not functioning or functionality is significantly impaired.
High	Major feature of product is not functioning or functionality is significantly impaired.
Medium	Minor feature of product is not functioning or functionality is significantly impaired.
Low	General question on functionality.

The priority of a case may be escalated based on current customer situation or overall satisfaction level of the customer.

### 7.1.2 Severity Level Examples

Severity	Examples
Critical	<p><u>Video Surveillance</u></p> <ul style="list-style-type: none"> <li>✓ Entire system is down and not operational</li> <li>✓ Video is not being recorded</li> </ul> <p><u>Access Control</u></p> <ul style="list-style-type: none"> <li>✓ None of the credential work</li> <li>✓ none of the doors are opening</li> <li>✓ Main doors don't open/lock</li> </ul> <p><u>License Plate Recognition</u></p> <ul style="list-style-type: none"> <li>✓ LPR System is not starting / not able to read plates / crashing frequently</li> <li>✓ Touch Screen is not functional</li> <li>✓ Autofind w/ chalking has no GPS</li> </ul>

	<ul style="list-style-type: none"> <li>✓ Right LPR / Tire camera is not working</li> <li>✓ Production database not accessible / not functional</li> <li>✓ Match process is not functional</li> <li>✓ IRWS is not functional / not able to connect to LPR Server(s)</li> <li>✓ Images are not displayed from IRWS</li> <li>✓ Not enough free space on the LPR Server(s)</li> <li>✓ LPR Server / Lane / IRWS computer is crashing frequently</li> </ul>
<p>High</p>	<p><u>General</u></p> <ul style="list-style-type: none"> <li>✓ Users unable to log in (AD)</li> <li>✓ Alarm Management not functioning</li> <li>✓ Services not being restarted by WD</li> <li>✓ Service crashes/restarts sporadically</li> <li>✓ Unable to launch client application</li> </ul> <p><u>Video Surveillance</u></p> <ul style="list-style-type: none"> <li>✓ Poor image quality</li> <li>✓ Video not recorded on a few cameras or large number of cameras not available</li> <li>✓ DFC not functioning</li> </ul> <p><u>Access Control</u></p> <ul style="list-style-type: none"> <li>✓ Secondary door does not open/lock</li> <li>✓ Synchronization problem</li> </ul> <p><u>License Plate Recognition</u></p> <ul style="list-style-type: none"> <li>✓ Hotlist not updated</li> <li>✓ Not able to offload</li> <li>✓ No wireless connection</li> <li>✓ GPS problem</li> <li>✓ Left LPR / Tire camera is not working</li> <li>✓ Mobile LPR System is working but on occasion it is crashing</li> <li>✓ Back-Office software is crashing</li> <li>✓ System is missing plates (less than 90 % read rate)</li> <li>✓ System is reading plates poorly (less than 70% perfect read)</li> </ul>

	<p>rate)</p> <ul style="list-style-type: none"> <li>✓ Review Server is not functional</li> <li>✓ Archive database is not created</li> <li>✓ Archive / Backup job is not enabled</li> <li>✓ Custom Replication is not enabled in a multi LPR Server environment</li> <li>✓ Images not pushed from lane computer to the LPR Server(s)</li> <li>✓ Lane computer is missing license plates (less than 90 % read rate)</li> <li>✓ Lane computer is reading license plates poorly (less than 70% perfect read rate)</li> <li>✓ Lane computer is not functional / able to capture license plates</li> <li>✓ Lane computer is not able to send transactions to the LPR Server(s).</li> <li>✓ Back-Office application is not functional on the IIS server</li> <li>✓ Back-Office application is unable to show open/closed transactions or to show images, with or without ActiveX control</li> <li>✓ Back-Office application unable to export to client / IIS computer</li> <li>✓ Lane computer is not able to send reviews</li> </ul>
<p>Medium</p>	<p><u>General</u></p> <ul style="list-style-type: none"> <li>✓ Licensing</li> <li>✓ PTZ functionality</li> <li>✓ USB Joystick functionality</li> <li>✓ Macros/plugin not functioning</li> <li>✓ DB problem</li> <li>✓ Unit occasionally not available</li> <li>✓ Cosmetic problems</li> <li>✓ Problem with some credential</li> </ul> <p><u>Access Control</u></p> <ul style="list-style-type: none"> <li>✓ Some controllers are offline</li> <li>✓ Badge designer issue</li> </ul> <p><u>License Plate Recognition</u></p>

	<ul style="list-style-type: none"> <li>✓ System is missing plates (more than 90% read rate)</li> <li>✓ System is reading plates poorly (more than 70% perfect read rate)</li> <li>✓ Hardware broken but system still can read plates</li> <li>✓ Missing functionality (Upgrade request)</li> <li>✓ Lane computer is missing plates (between 90% and 95% read rate)</li> <li>✓ Lane computer is reading plates poorly (between 70% and 80% perfect read rate)</li> </ul>
Low	<ul style="list-style-type: none"> <li>✓ Feature requests</li> <li>✓ General question</li> </ul>

## 7.2 Response Times

### 7.2.1 First Response

GTAC will respond to all new calls placed within the following time frames:

Call Entry Point	Response Time
Phone call	15 minutes <sup>1/2</sup>
GTAP	1 business day

<sup>1</sup>: Phone calls placed outside the scope of the customer's support agreement will be returned first thing on Genetec's next business day.  
<sup>2</sup>: GTAC objectives are 3 minutes average speed to answer and to answer 90% of calls within 10 minutes.

### 7.2.2 Status Updates

GTAC will provide continuous updates on the status of the troubleshooting based on the severity and priority of the case as detailed in the table below.

	In Progress (hours) <sup>1</sup>	Customer Action Required (days) <sup>1</sup>
Critical	4	1
High	24	1
Medium	48	3
Low	72	5

<sup>1</sup>: Status updates are provided within regular GTAC business hours.

**7.2.3 Three Strike Rule - Follow up**

The GTAC will follow up with customers for cases in the Customer Response Pending (CRP) state according to the table above in order to ensure timely resolution of issues.

For low and medium severity cases, the GTAC will follow up 3 times at intervals of 3 business days. After 3 consecutive and unsuccessful attempts, the ticket will be automatically closed.

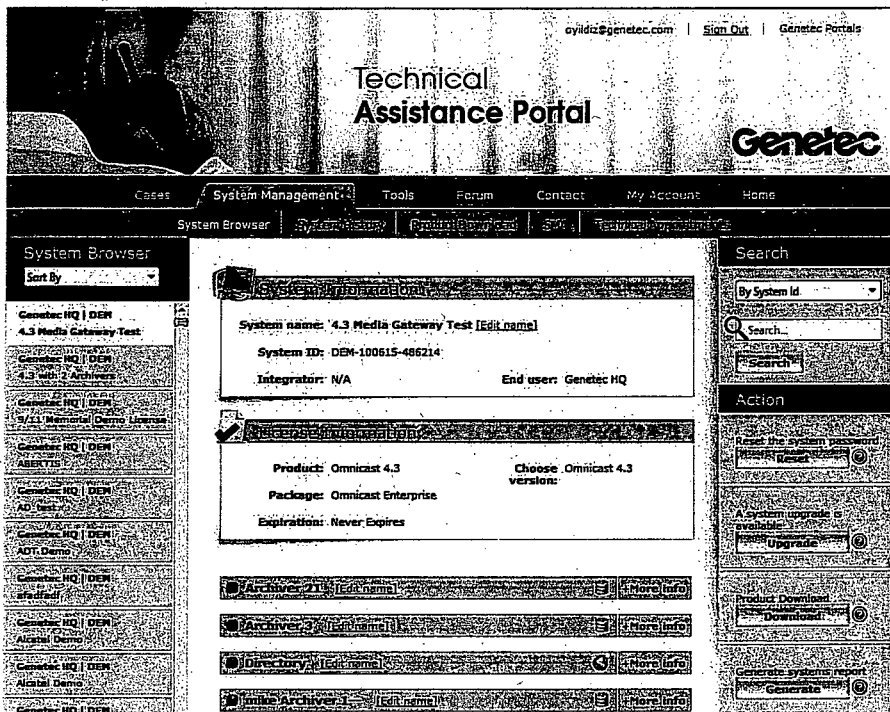
For high and critical severity cases, the GTAC will follow up 3 times at intervals of 1 business day. After 3 consecutive and unsuccessful attempts, the priority of the case will be lowered to medium severity and the cycle will start again as detailed above.

**7.3 Resource Commitment**

Genetec cannot guarantee a resolution time for issues but can guarantee resources committed to fixing the problem. The following table details the resource commitment based on the severity of the case.

<b>Severity</b>	<b>Resource Commitment</b>
<b>Critical</b>	Full-time resource around the clock
<b>High</b>	Full-time resource within business hours
<b>Medium</b>	Based on availability with a priority over Low
<b>Low</b>	No commitment

## 8 The Genetec Technical Assistance Portal



### 8.1 Accessing the GTAP

GTAP access is currently reserved to Genetec's customers and partners. In order to access the GTAP, you will need the following:

1. System ID and Password
  - This will only give access to the System Management (license) section of the portal for the provided System ID.
2. User Credential and Password
  - This will give full access to the Portal.
  - To Register use the following link: <https://gtap.genetec.com/Register.aspx>

## 8.2 Available Resources

### 8.2.1 System Management (Licenses)

The GTAP allows you to manage your system licenses without the intervention of a GTAC representative by:

- Resetting your system password
- Resetting your license
- Upgrading your system
- Downloading the newest product version
- Generating systems reports

### 8.2.2 GTAC Case Management

GTAP case management system allows you to manage your GTAC support cases by:

- Creating new support cases
- Browsing through opened and closed support cases
- Taking ownership of support cases in your organization
- Updating support cases and attaching files to them
- Escalating support cases to GTAC leadership
- Requesting call backs on support cases
- Closing/resolving open support cases

### 8.2.3 Documentation and Knowledge Base

The GTAP is also a repository for considerable amounts of documentation such as release notes, installations guides, user guides, tutorials, application notes, and much more. It is also a repository for a continuously updated knowledge base that contains hundreds of articles that will help you troubleshoot your system.

### 8.2.4 Video and Webinars

The GTAP is also a repository of other multimedia items such as videos. On the GTAP, you will find short tutorial videos (GTAC Tech Tube), monthly webinar archives (GTAC Tech Talk) and computer based training courses that will enable you to increase your knowledge on Genetec's products and solutions.

### **8.2.5 Community Forums**

GTAP users also form a community and share on the GTAP forums. A variety of topics regarding best practices, issues and installations are discussed on the community forums.

### **8.2.6 Arrange for Technical Appointments**

Planning for an upgrade and need the assistance of a GTAC representative? The GTAP allows you to arrange for technical appointments included in your SMA.

### **8.2.7 Supported Device Tool**

The GTAP's Support Devices tool gives you access to Genetec's comprehensive compatibility database that contains valuable information on which third party devices are supported on which version of Genetec software with which version of firmware. When available, the latest firmwares are published on this tool and available for download.

### **8.2.8 Known Issues**

On the GTAP, the known issues lists will provide you with insight on possible issues that may affect your system. From this list, you will know if there are any workarounds in knowledge base articles or hotfixes. You will also know in which version the known issue is fixed and you can also request a hotfix for your version.

### **8.2.9 GTAC Monthly Minute**

The GTAC Monthly Minute is your one-stop update on all that is happening in the GTAC. This monthly newsletter keeps you up to date with new product releases, GTAP updates and GTAC news. Subscribing to this newsletter is the best way to stay informed about what is new in the GTAC.



## 9 Appendix A – Software Warranty Lengths

Product Family	Standard Warranty Length
Omnicast	1 year
Omnicast (Upgrade)	90 Days
Security Center	1 years
Security Center (Upgrade)	90 days
Security Center Mobile	1 years
Security Center Mobile (Upgrade)	90 days
Plan Manager	1 year
Plan Manager (Upgrade)	90 days
SV-16	2 years
SV-16 (Upgrade)	90 Days
Custom Developed Software	60 Days

## 10 Appendix B – Hardware Warranty Lengths

Product Family	Standard Warranty Length	Maximum Extended Warranty Length (in addition to standard warranty)
AutoVu Sharp	1 year	4 years
SV-16	2 years	n/a
HID VeriX	18 Months	n/a
HID Edge	18 Months	n/a

APPENDIX *GH*

**EQUIPMENT ACCEPTANCE CERTIFICATE**

The undersigned purchaser hereby acknowledges receipt of the equipment order described below. After confirmation of order fulfillment, and on-site product testing, we are now accepting the equipment as satisfactory for all purposes in accordance with the Agreement.

Quantity	Model Number	Equipment Description

\_\_\_\_\_  
City of Berkeley Representative/Position

\_\_\_\_\_  
Date

END OF SECTION

**DEPARTMENT ORDER****ADMINISTRATIVE ORDER #001-2015****DATE ISSUED: 01/5/15****SUBJECT: AUTOMATED LICENSE PLATE READER USE****PURPOSE:**

This order establishes guidelines for the use of the Berkeley Police Department's Automated License Plate Reader (ALPR) technology and data. ALPR technology functions by automatically capturing an image of a vehicle's license plate, transforming that image into alphanumeric characters using optical character recognition software, and storing that information, along with relevant metadata (e.g. geo-location and temporal information, as well as data about the ALPR unit). ALPRs may be used by the Berkeley Police Department Parking Enforcement and Traffic Units for official law enforcement purposes. This Administrative Order shall remain in effect until January 6, 2016, or when superseded by the issuance of a General Order governing ALPR use.

**ADMINISTRATION OF ALPR DATA:**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain through the Parking Enforcement Unit. The Investigations Division Captain will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

**ALPR OPERATION:**

Use of an ALPR is described below. Department personnel shall not use, or allow others to use the equipment or database records for any unauthorized purpose.

- a. An ALPR shall only be used for official and legitimate law enforcement business.
- b. Reasonable suspicion or probable cause is not required before using an ALPR.
- c. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- d. No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.

**ALPR DATA COLLECTION AND RETENTION:**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department, and because such data may contain confidential CLETS information, are not open to public review. ALPR information gathered and

retained by this department may be used and shared with prosecutors or others only as permitted by law.

The Parking Enforcement Manager is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by City Department of Information Technology personnel.

All ALPR data shall be stored and purged as described below in this order and thereafter shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data shall be downloaded from the server onto portable media and booked into evidence.

**ACCOUNTABILITY AND SAFEGUARDS:**

All saved data will be closely safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data:

- a. Non-law enforcement requests for access to stored ALPR data shall be referred to the Public Safety Business Manager and processed in accordance with applicable law.
- b. Non-law enforcement requests for information regarding a specific vehicle's license plate shall be honored when the requestor is the registered owner of the vehicle in question. The requestor in such cases must provide acceptable proof of their identity and of their ownership of the vehicle in question.
- c. ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.
- d. Berkeley Police personnel approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- e. ALPR data may be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes only in connection with specific criminal investigations.
- f. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state, or federal agency or entity without the express written consent of the City Manager.
- g. For purposes of a City of Berkeley Parking Enforcement analysis effort, ALPR data may be provided a City of Berkeley consultant on an as-needed basis, upon the specific approval of the Chief of Police or his/her designee.
- h. ALPR system audits should be conducted by personnel assigned to the Professional Standards Bureau on a regular basis, at least biennially.

- i. ALPR "read" data retention periods may vary, depending on the system using the ALPR. Regardless of system use, all ALPR "read" data shall be retained for no longer than 365 days, after which point it shall be automatically purged from the server or storage device.

**CURRENT ALPR DEPLOYMENT-SCOFFLAW ENFORCEMENT:**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for Scofflaw Enforcement. The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and checks scanned "reads" against a file of vehicles which have five or more outstanding citations. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car. This allows the city to recover outstanding citation fees and penalties.

ALPR equipment is installed in the Parking Enforcement Unit's Scofflaw Enforcement vehicle and a marked Traffic Enforcement vehicle, allowing for scofflaw enforcement using both vehicles.

The contracted vendor for the City's Scofflaw Enforcement program is Paylock. Paylock stores data on a secure server, and provides access to authorized personnel Paylock's "Bootview" secure website, as described below:

- a. All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

When a car is booted and/or towed, the read, hit, and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.



Michael K. Meehan  
Chief of Police

cc: All BPD Personnel



City of Berkeley  
Abstract of Bid Worksheet

Finance Department  
General Services Division

FOR: Equipment for Automated Parking  
Data Collection + Enforcement

Spec. # 14-10825-C

Bid Date: 8/21/14

	Bidders	Base Bid	Nuc Free	Work Force Comp	Opp. States	Living Wage	EBO	Bid Bond	Addenda
1	PCS Mobile								
2	Tannery Creek Systems		X	X	X	X	X		
3									
4									
5									
6									
7									
8									
9									
10									

Bid Recorder: Shelley Goss 8/21

Bid Opener: STB 8/21/14

Project Manager: [Signature] 8/25/14

2180 McKia Street, Berkeley, CA 94704 Tel: 510.981.7320 TDD: 510.981.6903 Fax: 510.981.7390  
E-mail: [finance@ci.berkeley.ca.us](mailto:finance@ci.berkeley.ca.us)

**NON-DISCRIMINATION/WORKFORCE COMPOSITION**

FOR ALL CONTRACTS: 5 OR MORE EMPLOYEES

To assist the City of Berkeley in implementing its Non-Discrimination policy, you're requested to furnish information regarding your personnel, as indicated below, and return this form to the City Department handling your contract.

**ORGANIZATION** Portable Computer Systems, Inc dba PCS Mobile  
**ADDRESS** 1200 W. Mississippi Ave, Denver, CO 80223  
**BUSINESS LICENSE #** \_\_\_\_\_

You may complete this online & make entries in these cells, they will be automatically totaled at the bottom; or print the form & complete by hand/typewriter.

Occupational Category (see page 2 for definitions)	ALL EMPLOYEES		WHITE		BLACK		ASIAN		HISPANIC		OTHER (specify)**	
	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
Officials/Administrators	1	1	1	1								
Professionals	2	0	0	0								
Technicians	15	0	6	0	1		2	0	6	0	0	0
Protective Service Workers	0	0										
Para-professionals	0	0										
Office/Clerical	0	0			3						3	
Skilled Craft Workers	0	0										
Service/Maintenance	0	0										
Other Occupation: Specify*	8	3	7	3							1	
<b>Totals</b>	<b>24</b>	<b>10</b>	<b>14</b>	<b>7</b>	<b>1</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>7</b>	<b>3</b>	<b>0</b>	<b>0</b>

\*Specify other occupation: FRST / MTS - CELL MGMT @ SALES WORKERS  
 \*\*Specify other ethnicity: \_\_\_\_\_

Is your business MBE/WBE/DBE certified?  YES  
 If Yes, by what agency? The Supplier Clearinghouse for the Utility Supplier Diversity Program  
 of the California Public Utilities Commission  
 Do you have a policy of non-discrimination?  YES  
 If Yes, please specify: WBE or ethnic identification: \_\_\_\_\_

Signature Steven McKay Date 4.2.15  
 Print/Type Name of Signer Steven McKay  
 Verified by \_\_\_\_\_ Date \_\_\_\_\_  
 City of Berkeley Contract Administrator



**CITY OF BERKELEY**  
**Nuclear Free Zone Disclosure Form**

I (we) certify that:

1. I am (we are) fully cognizant of any and all contracts held, products made or otherwise handled by this business entity, and of any such that are anticipated to be entered into, produced or handled for the duration of its contract(s) with the City of Berkeley. (To this end, more than one individual may sign this disclosure form, if a description of which type of contracts each individual is cognizant is attached.)
2. I (we) understand that Section 12.90.070 of the Nuclear Free Berkeley Act (Berkeley Municipal Code Ch. 12.90; Ordinance No. 5784-N.S.) prohibits the City of Berkeley from contracting with any person or business that knowingly engages in work for nuclear weapons.
3. I (we) understand the meaning of the following terms as set forth in Berkeley Municipal Code Section 12.90.130:  
  

"Work for nuclear weapons" is any work the purpose of which is the development, testing, production, maintenance or storage of nuclear weapons or the components of nuclear weapons; or any secret or classified research or evaluation of nuclear weapons; or any operation, management or administration of such work.

"Nuclear weapon" is any device, the intended explosion of which results from the energy released by reactions involving atomic nuclei, either fission or fusion or both. This definition of nuclear weapons includes the means of transporting, guiding, propelling or triggering the weapon if and only if such means is destroyed or rendered useless in the normal propelling, triggering, or detonation of the weapon.

"Component of a nuclear weapon" is any device, radioactive or non-radioactive, the primary intended function of which is to contribute to the operation of a nuclear weapon (or be a part of a nuclear weapon).
4. Neither this business entity nor its parent nor any of its subsidiaries engages in work for nuclear weapons or anticipates entering into such work for the duration of its contract(s) with the City of Berkeley.

Based on the foregoing, the undersigned declares under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Printed Name: Steven McKay Title: Treasurer

Signature: *Steven McKay* Date: 4.2.2015

Business Entity: Portable Computer Systems, Inc dba PCS Mobile

Contract Description/Specification No. License Plate Recognition System & Services  
Attachment C

**CITY OF BERKELEY**  
**Oppressive States Compliance Statement for Personal Services**

The undersigned, an authorized agent of Portable Computer Systems, Inc dba PCS Mobile (hereafter "Vendor"), has had an opportunity to review the requirements of Berkeley City Council Resolution No. 59,853-N.S. (hereafter "Resolution"). Vendor understands and agrees that the City may choose with whom it will maintain business relations and may refrain from contracting with those Business Entities which maintain business relationships with morally repugnant regimes. Vendor understands the meaning of the following terms used in the Resolution:

"Business Entity" means "any individual, firm, partnership, corporation, association or any other commercial organization, including parent-entities and wholly-owned subsidiaries" (to the extent that their operations are related to the purpose of the contract with the City).

"Oppressive State" means: **Tibet Autonomous Region and the Provinces of Abo, Kham, and U-Tsang.**

"Personal Services" means "the performance of any work or labor and shall also include acting as an independent contractor or providing any consulting advice or assistance, or otherwise acting as an agent pursuant to a contractual relationship."

Contractor understands that it is not eligible to receive or retain a City contract if at the time the contract is executed, or at any time during the term of the contract it provides Personal Services to:

- a. The governing regime in any Oppressive State.
- b. Any business or corporation organized under the authority of the governing regime of any Oppressive State.
- c. Any person for the express purpose of assisting in business operations or trading with any public or private entity located in any Oppressive State.

Vendor further understands and agrees that Vendor's failure to comply with the Resolution shall constitute a default of the contract and the City Manager may terminate the contract and bar Vendor from bidding on future contracts with the City for five (5) years from the effective date of the contract termination.

The undersigned is familiar with, or has made a reasonable effort to become familiar with, Vendor's business structure and the geographic extent of its operations. By executing the Statement, Vendor certifies that it complies with the requirements of the Resolution and that if any time during the term of the contract it ceases to comply, Vendor will promptly notify the City Manager in writing.

Based on the foregoing, the undersigned declares under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Printed Name: Steven McKay Title: Treasurer

Signature: *Steven McKay* Date: 4.2.2015

Business Entity: Portable Computer Systems, Inc dba PCS Mobile

I am unable to execute this Statement; however, Vendor is exempt under Section VII of the Resolution. I have attached a separate statement explaining the reason(s) Vendor cannot comply and the basis for any requested exemption.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Contract Description/Specification No.: License Plate Recognition System & Services

Attachment D

CITY OF BERKELEY  
Living Wage Certification for Providers of Personal Services

**TO BE COMPLETED BY ALL PERSONS OR ENTITIES ENGAGING IN A CONTRACT FOR PERSONAL SERVICES WITH THE CITY OF BERKELEY.**

The Berkeley Municipal Code Chapter 13.27, Berkeley's Living Wage Ordinance (LWO), provides that contractors who engage in a specified amount of business with the City (except where specifically exempted) under contracts which furnish services to or for the City in any twelve (12) month period of time shall comply with all provisions of this Ordinance. The LWO requires a City contractor to provide City mandated minimum compensation to all eligible employees, as defined in the Ordinance. In order to determine whether this contract is subject to the terms of the LWO, please respond to the questions below. Please note that the LWO applies to those contracts where the contractor has achieved a cumulative dollar contracting amount with the City. Therefore, even if the LWO is inapplicable to this contract, subsequent contracts may be subject to compliance with the LWO. Furthermore, the contract may become subject to the LWO if the status of the Contractor's employees change (i.e. additional employees are hired) so that Contractor falls within the scope of the Ordinance.

**Section I.**

**1. IF YOU ARE A FOR-PROFIT BUSINESS, PLEASE ANSWER THE FOLLOWING QUESTIONS**

a. During the previous twelve (12) months, have you entered into contracts, including the present contract, bid, or proposal, with the City of Berkeley for a cumulative amount of \$25,000.00 or more?

YES  NO

If no, this contract is NOT subject to the requirements of the LWO, and you may continue to Section II. If yes, please continue to question 1(b).

b. Do you have six (6) or more employees, including part-time and stipend workers?

YES  NO

If you have answered, "YES" to questions 1(a) and 1(b) this contract IS subject to the LWO. If you responded "NO" to 1(b) this contract IS NOT subject to the LWO. Please continue to Section II.

**2. IF YOU ARE A NON-PROFIT BUSINESS, AS DEFINED BY SECTION 501(C) OF THE INTERNAL REVENUE CODE OF 1954, PLEASE ANSWER THE FOLLOWING QUESTIONS.**

a. During the previous twelve (12) months, have you entered into contracts, including the present contract, bid or proposal, with the City of Berkeley for a cumulative amount of \$100,000.00 or more?

YES  NO

If no, this Contract is NOT subject to the requirements of the LWO, and you may continue to Section II. If yes, please continue to question 2(b).

b. Do you have six (6) or more employees, including part-time and stipend workers?

YES  NO

If you have answered, "YES" to questions 2(a) and 2(b) this contract IS subject to the LWO. If you responded "NO" to 2(b) this contract IS NOT subject to the LWO. Please continue to Section II.

**Section II**

Please read, complete, and sign the following:

THIS CONTRACT IS SUBJECT TO THE LIVING WAGE ORDINANCE.

THIS CONTRACT IS NOT SUBJECT TO THE LIVING WAGE ORDINANCE.

The undersigned, on behalf of himself or herself individually and on behalf of his or her business or organization, hereby certifies that he or she is fully aware of Berkeley's Living Wage Ordinance, and the applicability of the Living Wage Ordinance, and the applicability of the subject contract, as determined herein. The undersigned further agrees to be bound by all of the terms of the Living Wage Ordinance, as mandated in the Berkeley Municipal Code, Chapter 13.27. If, at any time during the term of the contract, the answers to the questions posed herein change so that Contractor would be subject to the LWO, Contractor will promptly notify the City Manager in writing. Contractor further understands and agrees that the failure to comply with the LWO, this certification, or the terms of the Contract as it applies to the LWO, shall constitute a default of the Contract and the City Manager may terminate the contract and bar Contractor from future contracts with the City for five (5) years from the effective date of the Contract termination. If the contractor is a for-profit business and the LWO is applicable to this contract, the contractor must pay a living wage to all employees who spend 25% or more of their compensated time engaged in work directly related to the contract with the City. If the contractor is a non-profit business and the LWO is applicable to this contract, the contractor must pay a living wage to all employees who spend 50% or more of their compensated time engaged in work directly related to the contract with the City.

These statements are made under penalty of perjury under the laws of the state of California.

Printed Name: Steven McKay Title: Treasurer

Signature: [Handwritten Signature] Date: 4.2.15

Business Entity: Portable Computer Systems, Inc dba PCS Mobile

Contract Description/Specification No: License Plate Recognition System and Services

Section III

• \*\* FOR ADMINISTRATIVE USE ONLY -- PLEASE PRINT CLEARLY \*\* •

I have reviewed this Living Wage Certification form, in addition to verifying Contractor's total dollar amount contract commitments with the City in the past twelve (12) months, and determined that this Contract IS / IS NOT (circle one) subject to Berkeley's Living Wage Ordinance.

Department Name

Department Representative

To be completed by  
Contractor/Vendor

Form EBO-1  
CITY OF BERKELEY



CERTIFICATION OF COMPLIANCE WITH EQUAL BENEFITS ORDINANCE

If you are a contractor, return this form to the originating department/project manager. If you are a vendor (supplier of goods), return this form to the Purchasing Division of the Finance Dept.

SECTION 1. CONTRACTOR/VENDOR INFORMATION

Name: Portable Computer Systems, Inc dba PCS Mobile Vendor No.:  
Address: 1200 W. Mississippi Ave City: Denver State: CO ZIP: 80223  
Contact Person: Steve McKay Telephone: 303-346-2487  
E-mail Address: stevem@pcsmobile.com Fax No.: 303-346-4274

SECTION 2. COMPLIANCE QUESTIONS

- A. The EBO is inapplicable to this contract because the contractor/vendor has no employees.
B. Does your company provide (or make available at the employees' expense) any employee benefits?
C. Does your company provide (or make available at the employees' expense) any benefits to the spouse of an employee?
D. Does your company provide (or make available at the employees' expense) any benefits to the domestic partner of an employee?
E. Are the benefits that are available to the spouse of an employee identical to the benefits that are available to the domestic partner of the employee?

SECTION 3. PROVISIONAL COMPLIANCE

- A. Contractor/vendor is not in compliance with the EBO now but will comply by the following date:
B. If you have taken all reasonable measures to comply with the EBO but are unable to do so, do you agree to provide employees with a cash equivalent?

\* The cash equivalent is the amount of money your company pays for spousal benefits that are unavailable for domestic partners.

SECTION 4. REQUIRED DOCUMENTATION

At time of issuance of purchase order or contract award, you may be required by the City to provide documentation (copy of employee handbook, eligibility statement from your plans, insurance provider statements, etc.) to verify that you do not discriminate in the provision of benefits.

**SECTION 5. CERTIFICATION**

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that I am authorized to bind this entity contractually. By signing this certification, I further agree to comply with all additional obligations of the Equal Benefits Ordinance that are set forth in the Berkeley Municipal Code and in the terms of the contract or purchase order with the City.

Executed this 2nd day of April, in the year 2015, at Denver, CO  
(City) (State)

Steven McKay  
Name (please print)

Steven McKay  
Signature

Treasurer  
Title

  
Federal ID or Social Security Number

**FOR CITY OF BERKELEY USE ONLY**

- Non-Compliant (The City may not do business with this contractor/vendor)
  - One-Person Contractor/Vendor       Full Compliance       Reasonable Measures
  - Provisional Compliance Category, Full Compliance by Date: \_\_\_\_\_
- Staff Name (Sign and Print): \_\_\_\_\_ Date: \_\_\_\_\_





**WORKERS COMPENSATION  
AND  
EMPLOYERS LIABILITY POLICY**

**ENDORSEMENT WC 00 03 13 (00)**

POLICY NUMBER: UB0CO67499

**WAIVER OF OUR RIGHT TO RECOVER FROM OTHERS ENDORSEMENT**

We have the right to recover our payments from anyone liable for an injury covered by this policy. We will not enforce our right against the person or organization named in the Schedule. (This agreement applies only to the extent that you perform work under a written contract that requires you to obtain this agreement from us.)

This agreement shall not operate directly or indirectly to benefit any one not named in the Schedule.

**SCHEDULE**

**DESIGNATED PERSON:**

**DESIGNATED ORGANIZATION:** City of Pasadena, its City Council, officers, officials, agents, employees, and volunteers.

DATE OF ISSUE: 6/9/2015

ST ASSIGN: California, Colorado



**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

## **TECHNOLOGY XTEND ENDORSEMENT**

This endorsement modifies insurance provided under the following:

### **COMMERCIAL GENERAL LIABILITY COVERAGE PART**

**GENERAL DESCRIPTION OF COVERAGE** – This endorsement broadens coverage. However, coverage for any injury, damage or medical expenses described in any of the provisions of this endorsement may be excluded or limited by another endorsement to this Coverage Part, and these coverage broadening provisions do not apply to the extent that coverage is excluded or limited by such an endorsement. The following listing is a general coverage description only. Limitations and exclusions may apply to these coverages. Read all the provisions of this endorsement and the rest of your policy carefully to determine rights, duties, and what is and is not covered.

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>A. Reasonable Force Property Damage – Exception To Expected Or Intended Injury Exclusion</li> <li>B. Non-Owned Watercraft Less Than 75 Feet</li> <li>C. Aircraft Chartered With Pilot</li> <li>D. Damage To Premises Rented To You</li> <li>E. Increased Supplementary Payments</li> <li>F. Who Is An Insured – Employees And Volunteer Workers – First Aid</li> <li>G. Who Is An Insured – Employees – Supervisory Positions</li> <li>H. Who Is An Insured – Newly Acquired Or Formed Organizations</li> <li>I. Blanket Additional Insured – Owners, Managers Or Lessors Of Premises</li> </ul> | <ul style="list-style-type: none"> <li>J. Blanket Additional Insured – Lessors Of Leased Equipment</li> <li>K. Blanket Additional Insured – Persons Or Organizations For Your Ongoing Operations As Required By Written Contract Or Agreement</li> <li>L. Blanket Additional Insured – Broad Form Vendors</li> <li>M. Who Is An Insured – Unnamed Subsidiaries</li> <li>N. Who Is An Insured – Liability For Conduct Of Unnamed Partnerships Or Joint Ventures</li> <li>O. Contractual Liability – Railroads</li> <li>P. Knowledge And Notice Of Occurrence Or Offense</li> <li>Q. Unintentional Omission</li> <li>R. Blanket Waiver Of Subrogation</li> </ul> |
|---|--|

### **PROVISIONS**

#### **A. REASONABLE FORCE PROPERTY DAMAGE – EXCEPTION TO EXPECTED OR INTENDED INJURY EXCLUSION**

The following replaces Exclusion a., **Expected Or Intended Injury**, in Paragraph 2., of **SECTION I – COVERAGES – COVERAGE A BODILY INJURY AND PROPERTY DAMAGE LIABILITY**:

##### **a. Expected Or Intended Injury Or Damage**

"Bodily injury" or "property damage" expected or intended from the standpoint of the insured. This exclusion does not apply to "bodily injury" or "property damage" resulting from the use of reasonable force to protect any person or property.

#### **B. NON-OWNED WATERCRAFT LESS THAN 75 FEET**

The following replaces Paragraph (2) of Exclusion g., **Aircraft, Auto Or Watercraft**, in Paragraph 2.

#### **of SECTION I – COVERAGES – COVERAGE A BODILY INJURY AND PROPERTY DAMAGE LIABILITY:**

(2) A watercraft you do not own that is:

- (a) Less than 75 feet long; and
- (b) Not being used to carry any person or property for a charge.

#### **C. AIRCRAFT CHARTERED WITH PILOT**

The following is added to Exclusion g., **Aircraft, Auto Or Watercraft**, in Paragraph 2. of **SECTION I – COVERAGES – COVERAGE A BODILY INJURY AND PROPERTY DAMAGE LIABILITY**:

This exclusion does not apply to an aircraft that is:

- (a) Chartered with a pilot to any insured;
- (b) Not owned by any insured; and
- (c) Not being used to carry any person or property for a charge.

## COMMERCIAL GENERAL LIABILITY

or volunteer doctor, in providing or failing to provide first aid or "Good Samaritan services" to a person.

2. The following is added to Paragraph 2.a.(1) of **SECTION II – WHO IS AN INSURED:**

Unless you are in the business or occupation of providing professional health care services, Paragraphs (1)(a), (b), (c) and (d) above do not apply to "bodily injury" arising out of providing or failing to provide first aid or "Good Samaritan services" by any of your "employees" or "volunteer workers", other than an employed or volunteer doctor. Any of your "employees" or "volunteer workers" providing or failing to provide first aid or "Good Samaritan services" during their work hours for you will be deemed to be acting within the scope of their employment by you or performing duties related to the conduct of your business.

3. The following is added to Paragraph 5. of **SECTION III – LIMITS OF INSURANCE:**

For the purposes of determining the applicable Each Occurrence Limit, all related acts or omissions committed by any of your "employees" or "volunteer workers" in providing or failing to provide first aid or "Good Samaritan services" to any one person will be deemed to be one "occurrence".

4. The following is added to the **DEFINITIONS** Section:

"Good Samaritan services" means any emergency medical services for which no compensation is demanded or received.

**G. WHO IS AN INSURED – EMPLOYEES – SUPERVISORY POSITIONS**

The following is added to Paragraph 2.a.(1) of **SECTION II – WHO IS AN INSURED:**

Paragraphs (1)(a), (b) and (c) above do not apply to "bodily injury" or "personal injury" to a co-"employee" in the course of the co-"employee's" employment by you arising out of work by any of your "employees" who hold a supervisory position.

**H. WHO IS AN INSURED – NEWLY ACQUIRED OR FORMED ORGANIZATIONS**

The following replaces Paragraph 4. of **SECTION II – WHO IS AN INSURED:**

4. Any organization you newly acquire or form, other than a partnership or joint venture, of which you are the sole owner

or in which you maintain the majority ownership interest, will qualify as a Named Insured if there is no other insurance which provides similar coverage to that organization. However:

- a. Coverage under this provision is afforded only:

(1) Until the 180th day after you acquire or form the organization or the end of the policy period, whichever is earlier, if you do not report such organization in writing to us within 180 days after you acquire or form it; or

(2) Until the end of the policy period, when that date is later than 180 days after you acquire or form such organization, if you report such organization in writing to us within 180 days after you acquire or form it, and we agree in writing that it will continue to be a Named Insured until the end of the policy period;

- b. Coverage A does not apply to "bodily injury" or "property damage" that occurred before you acquired or formed the organization; and

- c. Coverage B does not apply to "personal injury" or "advertising injury" arising out of an offense committed before you acquired or formed the organization.

**I. BLANKET ADDITIONAL INSURED – OWNERS, MANAGERS OR LESSORS OF PREMISES**

The following is added to **SECTION II – WHO IS AN INSURED:**

Any person or organization that is a premises owner, manager or lessor is an insured, but only with respect to liability arising out of the ownership, maintenance or use of that part of any premises leased to you.

The insurance provided to such premises owner, manager or lessor does not apply to:

- a. Any "bodily injury" or "property damage" caused by an "occurrence" that takes place, or "personal injury" or "advertising injury" caused by an offense that is committed, after you cease to be a tenant in that premises; or

dient, part or container entering into, accompanying or containing such products; or

- b. Any vendor for which coverage as an additional insured specifically is scheduled by endorsement.

**M. WHO IS AN INSURED – UNNAMED SUBSIDIARIES**

The following is added to **SECTION II – WHO IS AN INSURED**:

Any of your subsidiaries, other than a partnership or joint venture, that is not shown as a Named Insured in the Declarations is a Named Insured if:

- a. You maintain an ownership interest of more than 50% in such subsidiary on the first day of the policy period; and
- b. Such subsidiary is not an insured under similar other insurance.

No such subsidiary is an insured for "bodily injury" or "property damage" that occurred, or "personal injury" or "advertising injury" caused by an offense committed:

- a. Before you maintained an ownership interest of more than 50% in such subsidiary; or
- b. After the date, if any, during the policy period that you no longer maintain an ownership interest of more than 50% in such subsidiary.

**N. WHO IS AN INSURED – LIABILITY FOR CONDUCT OF UNNAMED PARTNERSHIPS OR JOINT VENTURES**

The following replaces the last paragraph of **SECTION II – WHO IS AN INSURED**:

No person or organization is an insured with respect to the conduct of any current or past partnership or joint venture that is not shown as a Named Insured in the Declarations. This paragraph does not apply to any such partnership or joint venture that otherwise qualifies as an insured under Section II – Who Is An Insured.

**O. CONTRACTUAL LIABILITY – RAILROADS**

1. The following replaces Paragraph c. of the definition of "insured contract" in the **DEFINITIONS** Section:
  - c. Any easement or license agreement;
2. Paragraph f.(1) of the definition of "insured contract" in the **DEFINITIONS** Section is deleted.

**P. KNOWLEDGE AND NOTICE OF OCCURRENCE OR OFFENSE**

The following is added to Paragraph 2., **Duties In The Event of Occurrence, Offense, Claim or Suit**, of **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS**:

- e. The following provisions apply to Paragraph a. above, but only for the purposes of the insurance provided under this Coverage Part to you or any insured listed in Paragraph 1. or 2. of Section II – Who Is An Insured:

- (1) Notice to us of such "occurrence" or offense must be given as soon as practicable only after the "occurrence" or offense is known to you (if you are an individual), any of your partners or members who is an individual (if you are a partnership or joint venture), any of your managers who is an individual (if you are a limited liability company), any of your trustees who is an individual (if you are a trust), any of your "executive officers" or directors (if you are an organization other than a partnership, joint venture, limited liability company or trust) or any "employee" authorized by you to give notice of an "occurrence" or offense.
- (2) If you are a partnership, joint venture, limited liability company or trust, and none of your partners, joint venture members, managers or trustees are individuals, notice to us of such "occurrence" or offense must be given as soon as practicable only after the "occurrence" or offense is known by:
  - (a) Any individual who is:
    - (i) A partner or member of any partnership or joint venture;
    - (ii) A manager of any limited liability company;
    - (iii) A trustee of any trust; or
    - (iv) An executive officer or director of any other organization;
 that is your partner, joint venture member, manager or trustee; or
  - (b) Any "employee" authorized by such partnership, joint venture, limited liability company, trust or other organization to give notice of an "occurrence" or offense.

RESOLUTION NO. 66,917-N.S.

CONTRACT: PCS MOBILE FOR EQUIPMENT PROVIDER OF AUTOMATED DATA COLLECTION AND ENFORCEMENT SYSTEM

WHEREAS, Public Works determined that an equipment vendor would be needed to test an alternative method of parking data collection for the Automated Data Collection and Enforcement system to support the goBerkeley pilot program; and

WHEREAS, in July 2014, the City of Berkeley released a Request for Qualifications for Specification No. 14-10875-C for an equipment vendor for the Automated Data Collection and Enforcement System, and received two valid proposals by the posted deadline; and

WHEREAS, after a thorough review and scoring according to the RFQ's criteria, as well as an on-site test and evaluation, the submission from PCS Mobile received a high overall score; and

WHEREAS, funding for this contract is available in the FY 2015 budget in the Federal Highway Administration Value Pricing Pilot Program (VPPP) Grant Fund (Fund 674), goBerkeley/FHWA restricted revenue portion of the Parking Meter Fund (Fund 840), and the remaining contract balance will be recommended for appropriation through the AAO No. 2 in the goBerkeley/FHWA restricted revenue portion of the Parking Meter Fund (Fund 840); the contract has been entered in the contract management database with CMS No. XUHAL.

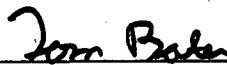
NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Manager is authorized to execute a contract and any amendments with PCS Mobile to provide equipment for the Automated Data Collection and Enforcement pilot portion of the goBerkeley program, for an amount not to exceed \$450,000 for the period March 1, 2015 through March 30, 2020. A record signature copy of said contract and any amendments to be on file in the City Clerk Department.

The foregoing Resolution was adopted by the Berkeley City Council on January 27, 2015 by the following vote:

Ayes: Anderson, Arreguin, Capitelli, Droste, Maio, Moore, Wengraf, Worthington and Bates.

Noes: None.

Absent: None.

  
\_\_\_\_\_  
Tom Bates, Mayor

Attest:   
\_\_\_\_\_  
Mark Numainville, City Clerk

CONSULTANTS APPENDIX<sup>1</sup>

Designated Employees

Disclosure Categories

Consultants who make (not just recommend) governmental decisions, such as whether to approve a rate, rule, or regulation, whether to issue, deny, suspend, or revoke any permit, license, application, certificate or similar authorization, adopt or grant City approval to a plan, design, report, study, or adopt or grant City approval of policies, standards, or guidelines for the City or any subdivision thereof

1

Consultants who act in a staff capacity with the City, and in that capacity perform the same or substantially all the same duties for the City that would otherwise be performed by an individual holding a designated position in the City's Conflict of Interest Code.

Disclosure required at the same level as the comparable designated position identified elsewhere in this Code.

Category 1

Designated consultants assigned to this category shall disclose:

- (a) All business entities or non-profit corporations in which they are a director, officer, partner, trustee, employee or hold a position of management; interests in real property, investments; and income, including gifts, loans and travel payments.<sup>2</sup>
- (b) When the consultant is a corporation or partnership, only individuals from the firm that participate in City decisions or act in a staff capacity must file disclosure statements.

<sup>1</sup> Only consultants who make a governmental decision or act in a staff capacity as defined in 2 Cal. Code Regs. Section 18701, as amended from time to time, shall be subject to economic disclosure requirements.

<sup>2</sup> Consultants who make governmental decisions shall disclose pursuant to the broadest disclosure category in the Code subject to the following limitation:

The chief executive officer may determine in writing that a particular consultant, although a "designated position," is hired to perform a range of duties that is limited in scope and thus is not required to fully comply with the disclosure requirements described in the section. Such written determination shall include a description of the consultant's duties and, based upon that description, a statement of the extent of disclosure requirements. The chief executive officer's determination is a public record and shall be retained for public inspection in the same manner and location as this Conflict of Interest Code.

EXHIBIT C

[View assistance for Search Results](#)

# Search Results

**Current Search Terms: personal\* computer\* systems\***

Your search for "Personal* Computer* Systems*" returned the following results...			
<small>Notice: This printed document represents only the first page of your SAM search results. More results may be available. To print your complete search results, you can download the PDF and print it.</small>			
Entity	<b>PERSONAL COMPUTER SYSTEMS, INC.</b>	Status: <b>Active</b>	
DUNS: 965216914	CAGE Code: 1GHM3	<input type="button" value="View Details"/>	
Has Active Exclusion?: No	DoDAAC:		
Expiration Date: 12/09/2015	Delinquent Federal Debt? Yes	<a href="#">What is this?</a>	
Purpose of Registration: All Awards			

### Glossary

#### Search Results

Entity

Exclusion

#### Search Filters

By Record Status

By Functional Area - Entity Management

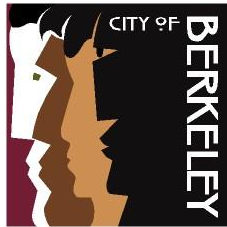
By Functional Area - Performance Information

SAM | System for Award Management 1.0

IBM v1.P.27.20150327-1711

**Note to all Users:** This is a Federal Government computer system. Use of this system constitutes consent to monitoring at all times.





Office of the City Manager

## **SUPPLEMENTAL AGENDA MATERIAL for Supplemental Packet 2**

**Meeting Date:** November 12, 2019

**Item Number:** 30

**Item Description:** Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras

**Submitted by:** Dee Williams-Ridley, City Manager

Attached is the originally published staff report with updated attachments. The staff report that was published did not include the surveillance technology reports. The following has been incorporated into the attachments:

- Surveillance Technology Report for Body Worn Cameras incorporated into Attachment 2.
- Surveillance Technology Report for Global Positioning System Tracking Devices incorporated into Attachment 3.
- Surveillance Technology Report for Automated License Plate Readers incorporated into Attachment 4.



Office of the City Manager

ACTION CALENDAR

November 12, 2019

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Andrew Greenwood, Chief of Police  
David White, Deputy City Manager

Subject: Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras

RECOMMENDATION

Adopt a Resolution accepting the Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras submitted pursuant to Chapter 2.99 of the Berkeley Municipal Code.

FISCAL IMPACTS OF RECOMMENDATION

There are no fiscal impacts associated with adopting the attached resolution.

CURRENT SITUATION AND ITS EFFECTS

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”). The purpose of the Ordinance is to provide transparency surrounding the use of surveillance technology, as defined by Section 2.99.020 in the Ordinance, and to ensure that decisions surrounding the acquisition and use of surveillance technology consider the impacts that such technology may have on civil rights and civil liberties. Further, the Ordinance requires that the City evaluate all costs associated with the acquisition of surveillance technology and regularly report on their use.

The Ordinance imposes various reporting requirements on the City Manager and staff. The purpose of this staff report and attached resolution is to satisfy annual reporting requirements as outlined in sections 2.99.050 and 2.99.070. The attached Surveillance Technology Reports, Surveillance Acquisition Reports and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras are for technologies that were acquired by the City prior to the adoption of the Ordinance.



Section 2.99.050 of the Ordinance required the City Manager to submit a Surveillance Acquisition Report and Surveillance Use Policy for each surveillance technology that has been possessed or used prior to the effective date of the Ordinance. The requirements of this section were not satisfied due to a multitude of factors, and the Police Department opted to submit the attached acquisition reports and use policies to the Police Review Commission prior to their review by the City Council. The Police Review Commission underwent an extensive engagement process and the full Commission discussed the attached use policies and reports at scheduled meetings from May to October 2019. In all cases, the Police Review Commission approved the attached acquisition reports and use policies and conveyed any concerns or suggested modifications to the Police Chief. In addition to the technologies covered by the attached resolution, City staff continues to evaluate whether or not there is any other technology that is used or possessed that is subject to the Ordinance.

Finally, Section 2.99.040 of the Ordinance allows the City Manager to borrow, acquire, or temporarily use surveillance technology in exigent circumstances without having to obtain the approval of City Council. Since the adoption of the ordinance, the City is reporting two instances in which the City Manager has made use of Section 2.99.040. In preparation for the potentially violent August 5, 2018 demonstration in downtown Berkeley, the City borrowed remote accessible cameras from the Northern California Regional Intelligence Center (NCRIC) in order to have the ability to remotely monitor intersections in real time. The cameras did not have face recognition technology. Signage was posted in the areas of the cameras, informing people that the area may be under video surveillance. Using cameras to monitor intersections is at times preferable to physically placing officers in those locations. In addition, as a mutual aid resource, the Police Department requested the Alameda County Sheriff's Office Small Unmanned Aerial System (sUAS) team as a mutual aid resource. The purpose of the request was to support the identification and apprehension of any felony suspects, should a felony occur. Following the felony vandalism of over ten City of Berkeley vehicles, the sUAS team deployed a drone, but no suspects were apprehended.

## BACKGROUND

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance. The Ordinance contains various reporting requirements including the following:

- Section 2.99.050, which requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the Ordinance; and

- Section 2.99.070 of the Ordinance, which requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November.

For each of the three technologies, the Surveillance Technology Report, Surveillance Acquisition Report and Surveillance Use Policies were prepared to satisfy the specific, section-by-section requirements of the Ordinance, and are attached to this report. It should be noted that substantial policies already existed for Body Worn Cameras and License Plate Readers. Those policies—also reviewed by the Police Review Commission for purposes of this report—are also attached. The existing policies will continue to remain in effect upon Council’s approval. Henceforth, all new Surveillance Use Policies and Surveillance Acquisition Reports will be listed in Chapter 13 of the Berkeley Police Department Policy Manual, which is being created to provide easy access to all policies relating to BMC 2.99. All BPD policies are available to the public on BPD’s website.

ENVIRONMENTAL SUSTAINABILITY

There are no identifiable environmental effects or opportunities associated with the content of this report.

RATIONALE FOR RECOMMENDATION

City Council is being asked to adopt the attached resolution for the City to be in compliance with the Ordinance.

ALTERNATIVE ACTIONS CONSIDERED

City Council could decide not to adopt the resolution or could direct staff to revise the attached policies.

CONTACT PERSON

Andrew Greenwood, Chief of Police, (510) 981-7017  
David White, Deputy City Manager, (510) 981-7012

ATTACHMENTS

1. Proposed Resolution

2. Body Worn Cameras

Surveillance Technology Report: Body Worn Cameras

Policy 1300 Body Worn Camera Use Policy

Policy 1300(a) Appendix: Body Worn Camera Acquisition Report

Policy 425 Body Worn Camera Policy (Existing Policy)

3. Global Positioning System Tracking Devices

Surveillance Technology Report

Policy 1301 Global Positioning System Tracking Devices Use Policy

Policy 1301(a) Appendix: Global Positioning System Tracking Devices Acquisition Report

4. Automated License Plate Readers

Surveillance Technology Report: Automated License Plate Readers

Policy 1302 Automated License Plate Reader Use Policy

Policy 1302(a) Appendix: Automated License Plate Reader Acquisition Report

Policy 422 Automated License Plate Reader (Latest version of existing Policy)

5. Police Review Commission Memorandum Regarding Automatic License Plate Readers

i:\surveillance ordinance\city council meeting -- 11-12-19\11-12-2019\_surveillance ordinance staff report and resolution (04).docx

RESOLUTION NO. ##,###-N.S.

A RESOLUTION ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT, SURVEILLANCE ACQUISITION REPORT, AND SURVEILLANCE USE POLICY FOR AUTOMATIC LICENSE PLATE READERS, GPS TRACKERS, AND BODY WORN CAMERAS

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”); and

WHEREAS, Section 2.99.050 of the Ordinance requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each piece of technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the Ordinance; and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Acquisition Reports and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras satisfy the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley:

Section 1. Pursuant to Section 2.99.060, as it pertains to the use of Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras, the City Council hereby finds and determines the following:

- a. The benefits of using the technologies outweigh the costs;
- b. The policies attached to this resolution safeguard civil liberties; and
- c. No feasible alternatives exist with similar utility that will have a lesser impact on civil rights or liberties.

Section 2. The City Council hereby accepts the Surveillance Technology Reports, Surveillance Acquisition Reports, and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras.

ATTACHMENT 2:  
BODY WORN CAMERAS

**Surveillance Technology Report: Body Worn Cameras**

**March 1, 2018 – Sept. 30, 2019**

<p>Description</p>	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Body Worn Cameras are used to capture video recordings of contacts between department personnel and the public, to provide an objective record of these events. These recording are used in support of criminal prosecutions, to limit civil liability, increase transparency and enhance professionalism and accountability in the delivery of police services to the community.</p> <p>Body Worn Camera files are shared with the Alameda County District Attorney’s office in support of prosecution for crime, and may be shared with other law enforcement agencies to support criminal investigations.</p> <p style="text-align: center;">Summary of Body Worn Camera Videos Uploaded March 1, 2018 to Sept. 30, 2019</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>Total Number of Videos</td> <td style="text-align: right;">42,677</td> </tr> <tr> <td>Total Hours of Videos</td> <td style="text-align: right;">10,681.93</td> </tr> <tr> <td>Total GB of Videos</td> <td style="text-align: right;">20,669.11</td> </tr> </table> <p style="text-align: center;">Summary of All Evidence Created March 1, 2018 to Sept. 30, 2019</p> <table style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th><u>Type</u></th> <th>Count of files</th> <th>Size (in Mb)</th> <th>GBs Storage</th> </tr> </thead> <tbody> <tr> <td>Audio</td> <td style="text-align: right;">2,315</td> <td style="text-align: right;">23,855.82</td> <td style="text-align: right;">23.86</td> </tr> <tr> <td>Document</td> <td style="text-align: right;">125</td> <td style="text-align: right;">17.56</td> <td style="text-align: right;">0.02</td> </tr> <tr> <td>Image</td> <td style="text-align: right;">64,931</td> <td style="text-align: right;">270,329.62</td> <td style="text-align: right;">270.33</td> </tr> <tr> <td>Other</td> <td style="text-align: right;">896</td> <td style="text-align: right;">118,080.19</td> <td style="text-align: right;">118.08</td> </tr> <tr> <td>Videos*</td> <td style="text-align: right;">70,670</td> <td style="text-align: right;">32,489,190.50</td> <td style="text-align: right;">32,489.19</td> </tr> <tr> <td>Grand Totals</td> <td style="text-align: right;">138,937</td> <td style="text-align: right;">32,901,473.69</td> <td style="text-align: right;">32,901.47</td> </tr> </tbody> </table> <p>* Includes all uploaded BWC videos <i>and</i> all other videos booked into the evidence management system. Other videos include iPhone videos uploaded, security camera video, copies of BWC videos (for redaction, etc.), and any other videos.</p>	Total Number of Videos	42,677	Total Hours of Videos	10,681.93	Total GB of Videos	20,669.11	<u>Type</u>	Count of files	Size (in Mb)	GBs Storage	Audio	2,315	23,855.82	23.86	Document	125	17.56	0.02	Image	64,931	270,329.62	270.33	Other	896	118,080.19	118.08	Videos*	70,670	32,489,190.50	32,489.19	Grand Totals	138,937	32,901,473.69	32,901.47
Total Number of Videos	42,677																																		
Total Hours of Videos	10,681.93																																		
Total GB of Videos	20,669.11																																		
<u>Type</u>	Count of files	Size (in Mb)	GBs Storage																																
Audio	2,315	23,855.82	23.86																																
Document	125	17.56	0.02																																
Image	64,931	270,329.62	270.33																																
Other	896	118,080.19	118.08																																
Videos*	70,670	32,489,190.50	32,489.19																																
Grand Totals	138,937	32,901,473.69	32,901.47																																
<p>Geographic Deployment</p>	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>Body Worn Cameras are worn by all BPD uniformed officers city-wide at all times; BWCs are not deployed based on geographic considerations.</p>																																		
<p>Complaints</p>	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There have been no complaints about the deployment and use of Body Worn Cameras.</p>																																		

<p><b>Audits and Violations</b></p>	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p> <p>File meta-data are routinely reviewed by our BWC manager, to ensure required meta-data fields are completed. There have been no complaints with regards to violations of the Surveillance Use Policy.</p>
<p><b>Data Breaches</b></p>	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There have been no known data breaches or other unauthorized access to BWC data.</p>
<p><b>Effectiveness</b></p>	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>Body Worn Cameras have proven effective in supporting criminal prosecutions, as video footage is available for all criminal prosecutions.</p> <p>Body Worn Cameras have been effective for training purposes, as footage can be reviewed in incident de-briefs.</p> <p>Body Worn Cameras have been extremely effective in support of Internal Affairs investigations and Use of Force Review.</p>
<p><b>Costs</b></p>	<p>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</p> <p>The annual cost for the Body Worn Cameras, including cameras, replacement cameras, software, and Axon's secure digital evidence management system is approx. \$204,000 per year over a five-year, \$1,218,000 contract. The systems cost for the 19 month period of this initial report was \$385,700.</p> <p>There is one full-time employee assigned to the BWC program, an Applications Programmer Analyst II, at a cost of \$168,940 per year, including benefits.</p>

## Surveillance Use Policy - Body Worn Cameras

### 1300.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department Body Worn Camera Policy #425 and adds elements as required by BMC 2.99.

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel. (Ref. policy 425.2)

### 1300.2 AUTHORIZED USE

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The BWC shall be activated in any of the following situations:

- (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- (c) Self-initiated field contacts in which a member would normally notify the Communications Center.
- (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
- (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.



At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation. (Ref. policy 425.7)

#### 1300.2.1 PROHIBITED USE

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule. (Ref. policy 425.13)

#### 1300.3 DATA COLLECTION

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. (Ref. policy 425.3)

#### 1300.4 DATA ACCESS

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 1300.4.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report. (Ref. policy 425.17)

##### 1300.4.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

- (a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed the video files.

---

It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
- (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
- (d) Prior to the conclusion of the criminal interview process, the involved member and/ or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.
- (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident." (Ref. policy 425.17.1)

#### 1300.4.2 SUPERVISORY REVIEW

With the exception of section 1300.4.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates. (Ref. policy 425.17.2)

#### 1300.4.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance. (Ref. policy 425.17.3)

- (a) Recorded files may also be reviewed:
  - 1. Upon approval by a supervisor, by any member of the Department who is participating

in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.

2. Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
3. By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
4. Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

(b) Investigators conducting criminal or internal investigations shall:

1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

#### 1300.4.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video. (Ref. policy 425.17.4)

#### 1300.4.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee. (Ref. policy 425.17.5)

### 1300.5 DATA PROTECTION

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. (Ref. policy 425.14)

---

### **1300.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of BWC data. These policies will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### **1300.7 DATA RETENTION**

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days. (Ref. policy 425.15)

### **1300.8 PUBLIC ACCESS**

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy. (Ref. policy 425.18)

### **1300.9 THIRD-PARTY DATA-SHARING**

#### **1300.9.1 CITY ATTORNEY**

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

---

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur. (Ref. policy 425.18)

#### 1300.9.2 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation. (Ref. policy 425.18.1)

- (a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

#### 1300.10 TRAINING

Training for the operation of BWC's shall be provided by BPD personnel. All BPD personnel who use BWC's shall be provided a copy of this Surveillance Use Policy.

#### 1300.11 AUDITING AND OVERSIGHT

Division Captains for divisions utilizing BWC's shall ensure compliance with this Surveillance Use Policy.

#### 1300.12 MAINTENANCE

The BWC system will be maintained by the Applications Programmer Analyst and assigned

Department of Information and Technology (IT) staff.

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18) (Ref policy 425.4):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.
- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.
- (h) All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

## 1300 APPENDIX A

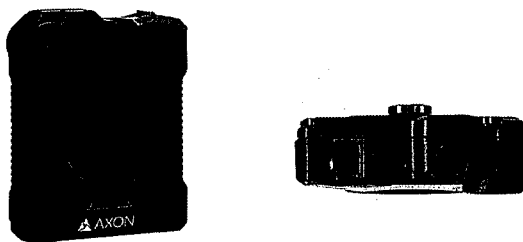
BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS

---

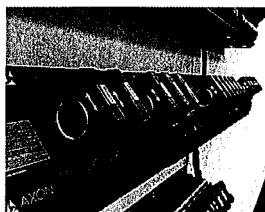
**BODY WORN CAMERAS (BWCs)****A. DESCRIPTION**

The BWC system consists of four main components: The camera, the docking station, and the Digital Information Management System (DIMS) and smartphone applications.

The first component, the Axon camera, is a system which incorporates an audio and video recording device. It is designed to record events in real time for secure storage, retrieval, and analysis. The camera is to be attached to an officer's uniform and is powered by an internal rechargeable battery. The camera features low-light performance, full-shift battery life, a capture rate of 30 frames per second with no dropped frames, HD video, pre-event buffering, multi-camera playback, and the ability to automatically categorize video using the police department's computer aided dispatch system. An officer can start and stop recording by pressing a button on the front of the camera. The camera does not contain a screen for footage review.



The second component of the system is the docking station. Once the Axon camera is placed in the docking station it recharges the camera's battery. The dock also triggers the uploading of data from the camera to a cloud based Digital Information Management System (DIMS) called Evidence.com. The dock does not directly provide functionality to view, modify or delete video data stored on Axon cameras.



The third component is the Digital Information Management System called Evidence.com. Evidence.com streamlines data management and sharing on one secure platform. The evidence management system is comprehensive, secure, and intuitive to use. The DIMS is located in a cloud-based data center for security, scalability, and ease of administration. Users can add

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

metadata to existing videos such as associated case numbers, incident type, incident dispositions, etc. to make the videos easier to find. However, the videos themselves cannot be altered by the user.

The fourth component of the system to be utilized are two Axon mobile applications, which allow officers to collect and review evidence in the field and more effectively use their BWCs. The applications use secure Bluetooth and Wi-Fi technology to access the BWC systems and footage. These applications are compliant with US Department of Justice evidentiary standards, meaning that they are both secure and are set up in a way that prohibits the altering or destruction of evidence. The applications are called Axon View and Axon Capture. Axon View allows users to change their camera settings, view live video, and review and tag recorded videos while they are stored on the BWC. Recorded videos remain in the BWC's memory, and cannot be manipulated or deleted. Axon Capture allows officers to use their city-issued smartphone's camera and microphone to take photographs, and record audio and video, and to upload this data directly to Evidence.com. These applications do not allow users to alter, manipulate, or edit any of the footage recorded by the BWC. These applications use secure technology to add value and efficiency to the BWC program.

**B. PURPOSE**

The primary objective of the BWC system is to document officer contacts, arrests, and critical incidents. Video footage collected by the BWCs will be used as evidence in both criminal and administrative investigations. Video footage not relevant to any investigation will be discarded after a defined retention period.

In instances where the officer might be expected to take law enforcement action of any kind, the officer is expected to record the encounter for the benefit of both the officer and the member of the public.

1. The BWC shall be activated in any of the following situations:
  - i. All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
  - ii. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
  - iii. Self-initiated field contacts in which a member would normally notify the Communications Center.
  - iv. Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.



**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

- v. Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- vi. Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is an officer expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the user can do so safely.

Officers should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Officers shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

2. Prohibited uses of the BWC system include:

- i. Officers shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.
- ii. Officers are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.
- iii. Officers are prohibited from retaining BWC recordings.
- iv. Officers shall not duplicate or distribute such recordings, except for department business purposes.

**C. LOCATION**

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers, in accordance with BPD policy #425.

**D. IMPACT**

With the introduction of BWCs, officers record all enforcement contacts with the public. To that end, an officer could find themselves engaged in their lawful duties in both public and private areas. Additionally, due to the nature of law enforcement work, an officer may be required to engage in sensitive conversations with individuals of all ages, including children.

The right to maintain someone's anonymity versus the need to gain information to maintain public safety is of paramount concern. The Department recognizes that all people have a right to privacy and is committed to protecting and safeguarding civil rights by adhering to the

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

strictest requirements of both state and federal law concerning release of audio/video recordings.

**E. MITIGATION**

In order to minimize violations of privacy, BWC policy provides that:

1. Officers should record any incident they feel would be appropriate or valuable to document. The BWC policy shall require officers to activate the BWC under the criteria listed above.
2. Officers should not activate the BWC and/or use caution when entering a public locker room, changing room, restroom, doctor's or attorney's office, or other place where individuals unrelated to the investigation are present and would have a heightened expectation of privacy unless the officer is investigating criminal activity or responding to a call for service.
3. BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy.
4. BWC footage will be retained or released in accordance with applicable state and federal law. Criminal defendants will have access to relevant BWC footage via the court discovery process.
5. Officers are prohibited from retaining BWC recordings, Officers shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.
6. Officers are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Officers may request restriction and subsequent deletion of an accidental recording according to the BWC policy.
7. Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted by law and department policy. Department policy does not authorize release of investigative files or documents that would constitute an unwarranted invasions of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy"

**F. DATA TYPES AND SOURCES**

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigations, and other proceedings protected by confidentiality laws and department policy.

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

The BWC collects video and audio recordings of events occurring in the user's presence. As each video is created, the system automatically stamps the video with the current date/time and the camera user's identity. The user has the option to add metadata manually to existing recordings after they are created. Such metadata may include but is not limited to:

1. Category of contact (from Department's defined list)
2. Disposition of contact (arrest, citation, etc.)
3. Associated case number

**G. DATA SECURITY**

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for transferring the data into the digital evidence management system. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings.

Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code Section 832.18) (Ref. policy 425.14):

1. Establishing a system for uploading, storing and security of recordings.
2. Designating persons responsible for uploading recorded data.
3. Establishing a maintenance system to ensure availability of BWCs.
4. Establishing a system for tagging and categorizing data according to the type of incident captured.
5. Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
6. Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
7. Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file,

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

**H. FISCAL COST**

In 2017, the Berkeley City Council approved a resolution authorizing a contract between BPD and Axon. Axon was chosen after a competitive Request for Proposal (RFP) process. The contract will not exceed \$1,218,103 and includes the cost of 200 body worn cameras, charging stations, accessories, software licenses, training and unlimited storage for five years. The purchase also includes replacement cameras and charging stations during the third and fifth year of the contract.

There will be an annual cost of approximately \$250,000 to the police department's budget for a staff person to administer the body worn camera program beginning in FY 2019.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

**J. ALTERNATIVES**

Officers rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, BPD sees the use of BWCs as an integral strategy to strengthen police transparency, prevent and resolve complaints against the police by civilians, document police-public interaction, and promote the perceived legitimacy and sense of procedural justice that communities have about their departments. There is a broad consensus – among community leaders, the ACLU, the Department of Justice, the Berkeley Police Department, and elected officials – that body-worn cameras can be an important tool for improving the high-quality public service expected of police officers.

1300 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS

---

**K. EXPERIENCE OF OTHER ENTITIES**

Numerous police agencies have adopted BWCs as a tool to help combat crime, to reduce citizen complaints and to reduce use of force situations. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration, [https://www.bja.gov/bwc/pdfs/14-005\\_Report\\_BODY\\_WORN\\_CAMERAS.pdf](https://www.bja.gov/bwc/pdfs/14-005_Report_BODY_WORN_CAMERAS.pdf) - pages 6-8, cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard, <https://www.bwccscorecard.org/>, provides an analysis of how scores of different police agencies have employed BWCs through a defined list of metrics.

## Body Worn Cameras

### 425.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable Body Worn Cameras (BWCs) by members of this department while in the performance of their duties.

This policy does not apply to non-BWC evidence, including other methods of audio or video recordings, interviews or interrogations conducted at any Berkeley Police Department facility, authorized undercover operations, wiretaps or eavesdropping (concealed listening devices).

### 425.2 POLICY

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel.

While recordings obtained from BWCs provide an objective record of events, it is understood that video recordings do not necessarily capture all events, activities and information, or reflect the full experience of the individual member(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events as perceived and recalled by the involved member. Specifically, it is understood that the BWC will capture information that may not have been seen and/or heard by the involved member and that the involved member may see and hear information that may not have been captured by the BWC.

### 425.3 CONFIDENTIALITY AND PROPER USE OF RECORDINGS

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

### 425.4 COORDINATOR

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.

## Berkeley Police Department

Law Enforcement Services Manual

*Body Worn Cameras*

---

- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

**425.5 MEMBER RESPONSIBILITIES**

Prior to going into service, each uniformed member who is assigned to wear a BWC will be responsible for making sure that he or she is equipped with a BWC issued by the Department, and that the BWC is in good working order. If the BWC is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor to permit the supervisor or other department employee to provide the member with a functioning BWC as soon as practicable. Uniformed members should wear the recorder in a conspicuous manner as prescribed by the Department, to provide a generally unobstructed camera view of contacts between members of the public and department members.

Members lawfully engaged in their duties as a police officer are not required to obtain consent from, or give notice to, members of the public, prior to recording with their BWC.

Upon the approval of the Chief of Police, or his/her designee, non-uniformed members lawfully engaged in their duties as a police officer may use an approved BWC.

Members are required to document the existence of a recording in any report or other official record of the contact, such as a CAD entry, including any instance where the member is aware that the BWC malfunctioned or the member deactivated the recording. In the event activity outlined in section 425.7 is not captured in whole or in part the member shall document this and explain in their report their understanding, if any, of why the footage was not captured in the recording.

**425.6 SUPERVISOR RESPONSIBILITIES**

At such time as the scene is considered secure and safe, the on-scene supervisor shall take immediate physical custody of involved officer's/officers' BWC when the device may have captured an incident involving an officer-involved shooting or use of force resulting in death or great bodily injury, and shall ensure the data is uploaded in a timely manner as prescribed by BPD policy

## Berkeley Police Department

Law Enforcement Services Manual

*Body Worn Cameras*

---

(Penal Code § 832.18). Supervisors may review relevant BWC video and audio files in the field in furtherance of their duties and responsibilities.

Supervisors shall also review relevant BWC recordings prior to submitting any administrative reports.

**425.7 ACTIVATION OF THE BODY WORN CAMERA**

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The BWC shall be activated in any of the following situations:

- (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- (c) Self-initiated field contacts in which a member would normally notify the Communications Center.
- (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
- (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.



## Berkeley Police Department

Law Enforcement Services Manual

*Body Worn Cameras*

---

**425.8 VICTIMS AND WITNESSES OF CRIMES; INFORMANTS**

In the event that an officer has the opportunity to record interviews of victims and witnesses of crimes, they shall consider the following:

- (a) **Witnesses:** In the event a crime witness or a member of the community wishes to report or discuss criminal activity anonymously, officers have the discretion to not record. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the witness's recorded statement. In cases where a witness requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
- (b) **Victims:** Upon request by the victim, officers have the discretion to not record the interview. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the victim's recorded statement. In cases where a victim requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
  - 1. **Domestic Violence Victims:** Members should attempt to record interviews of domestic violence victims to facilitate future prosecution efforts and discourage later recanting of statements. Members should also record interviews with children who witness domestic violence, when the child is willing.
  - 2. **Child Abuse and Sexual Assault Victims:** Members shall have the discretion to record, absent any request to not record the interview by victims, witnesses, or non-suspect parents of victims, during child abuse and/or sexual assault investigations.
- (c) **Informants:** Members shall not activate their recorders when conducting an interview or engaging in a conversation with a confidential informant, unless needed as evidence.

Members have no obligation to advise a victim or witness that he or she is being recorded, but may do so at their discretion. When a victim or witness requests they not be recorded, members may consider their request (See Penal Code 632).

Members shall remain sensitive to the dignity of all individuals being recorded and exercise discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy concerns may outweigh any legitimate law enforcement interest in recording. Recording should resume when privacy concerns are no longer at issue unless the member determines that the circumstances no longer fit the criteria for recording.

Informal community interactions differ from "consensual encounters" in which members make an effort to develop reasonable suspicion to detain or probable cause to arrest. To strengthen relationships between police and citizens, members may use discretion regarding the recording of informal, non-enforcement related interactions with members of the community.

## Berkeley Police Department

Law Enforcement Services Manual

*Body Worn Cameras*

---

**425.9 ACTIVATION IN CROWD CONTROL SITUATIONS**

During crowd control, protest or mass arrest incidents, members shall use their BWCs consistent with this policy, or when directed by the Incident Commander. The Incident Commander shall document his or her orders to activate in an appropriate report (e.g. Operations Plan or After Action Report).

The limitations outlined in the Intelligence Procedures for First Amendment Activities Policy governing intelligence-gathering procedures for First Amendment activities, apply to the use of BWCs and other recording devices.

Video recording of individuals who are picketing or engaged in peaceful protest will be avoided unless the officer believes a violation of criminal law is occurring, may occur, or if the officer interacts with a participant or third party to the event, or a participant or third party initiates contact with the member.

**425.10 SURREPTITIOUS USE OF THE BWC**

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.

Members are prohibited from using department-issued BWCs for non-work related personal activity. BWCs will not be activated in places where members have a reasonable expectation of privacy, such as workplace locker rooms, dressing rooms, members' private vehicles or restrooms.

**425.11 CESSATION OF RECORDING**

Once activated, the member may mute or deactivate their BWC at any time based on their discretion, in the following circumstances:

- (a) Discussion of tactical or confidential information with other law enforcement personnel.
- (b) Where members are on a perimeter or assigned to a static post where the member's direct participation in the incident is complete and they are not actively part of an investigation.
- (c) If it is necessary to discuss issues or concerns with an employee, supervisor, doctor, nurse, or paramedic in private.
- (d) In the member's judgment, a recording would interfere with his or her ability to conduct an investigation.

Decisions regarding the reason for muting or BWC deactivation shall be noted on the recording, or otherwise documented.

## Berkeley Police Department

## Law Enforcement Services Manual

*Body Worn Cameras*

---

Members shall cease audio/video recording whenever necessary to ensure conversations are not recorded between a person in custody and the person's attorney, religious advisor or physician, unless there is explicit consent from all parties to the conversation. This does not apply to conversations with paramedics or EMTs during their response at a scene, and during transport.

**425.12 EXPLOSIVE DEVICE**

Many portable recorders, including BWCs and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

Members believing that the use of a BWC may detonate an explosive device may deactivate their BWC in such cases.

**425.13 PROHIBITED USE OF BODY WORN CAMERAS**

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Members may not use personally owned recorders (e.g. personal cell phone) to document contacts unless exigent circumstances exist to warrant the use of personally owned recording devices. Regardless, if a member is using a department-issued BWC, and/or another recording device, members shall comply with the provisions of this policy, including retention and release requirements. In every event where members use any recording device aside from or in addition to their department-issued BWC, the member shall document and explain the use and the exigent circumstance in their police report (e.g. the BWC failed and evidence needed to be captured at that moment in time).

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule.

**425.14 PROCESSING AND HANDLING OF RECORDINGS**

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

## Berkeley Police Department

## Law Enforcement Services Manual

*Body Worn Cameras*

---

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Members may request restriction and subsequent deletion of an accidental recording as described under section 425.16 below.

**425.15 RETENTION REQUIREMENTS**

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days.

**425.16 ACCIDENTAL RECORDING - REQUEST FOR RESTRICTION**

In the event of an accidental or sensitive personal recording of non-departmental business activity, where the resulting recording is of no investigative or evidentiary value, the recording employee may request that the file be restricted pending 60-day deletion by submitting an email request via their chain of command to the Professional Standards Division Captain. The Professional Standards Division Captain will approve or deny the restriction request. In cases where the request is denied, an appeal may be submitted to the Chief of Police, or his/her designee, for restriction authorization. In all cases of restriction requests, a determination should be made within seven calendar days.

**425.17 REVIEW OF RECORDINGS BY A MEMBER**

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 425.17.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report.

**425.17.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH**

- (a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed

## Berkeley Police Department

Law Enforcement Services Manual

Body Worn Cameras

---

the video files. It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
- (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
- (d) Prior to the conclusion of the criminal interview process, the involved member and/or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.
- (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officer(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident."

#### 425.17.2 SUPERVISORY REVIEW

With the exception of section 425.17.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates.

# Berkeley Police Department

## Law Enforcement Services Manual

### *Body Worn Cameras*

---

#### 425.17.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance.

Recorded files may also be reviewed:

- (a) Upon approval by a supervisor, by any member of the Department who is participating in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.
- (b) Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
- (c) By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
- (d) Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

Investigators conducting criminal or internal investigations shall:

1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

#### 425.17.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video.

#### 425.17.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee.

#### **425.18 RELEASE OF RECORDINGS**

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

## Berkeley Police Department

Law Enforcement Services Manual

Body Worn Cameras

---

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur.

**425.18.1 POLICE REVIEW COMMISSION (PRC)**

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation.

- (a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

**425.18.2 PUBLIC RECORDS ACT (PRA) REQUEST**

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

## Berkeley Police Department

Law Enforcement Services Manual

### *Body Worn Cameras*

---

#### 425.18.3 MEDIA

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy.

#### **425.19 COMPLIANCE WITH BMC 2.99 ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY**

This policy shall comply at all times with the requirement of BMC 2.99 Acquisition and Use of Surveillance Technology.

#### **425.20 TRAINING REQUIRED**

Officers who are assigned BWCs must complete department-approved training in the proper use and maintenance of the devices before deploying to the field.

As part of a continual improvement process, regular review should be conducted by BPD staff of the training on this policy and the related use of BWCs under this policy. Information resulting from the outcomes of this review shall be incorporated into the City Manager's annual "Surveillance Technology Report" as required under BMC 2.99 Acquisition and Use of Surveillance Technology.

The Department, Police Review Commission and other City Departments shall maintain the confidentiality of Department sworn employee personnel records as required by state and local law. Failure to maintain the confidentiality of Department sworn employee personnel records, whether or not intentional, may subject individuals to civil penalties and discipline, up to and including termination of employment.



**ATTACHMENT 3:**  
**Global Positioning System Tracking Devices**

## Surveillance Technology Report: Global Positioning System Tracking Devices

March 1, 2018 – Sept. 30, 2019

Description	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Global Positioning System Trackers are used to track the movements of vehicles, bicycles, other items, and/or individuals for the purpose of investigating criminal activity.</p> <p>Global Positioning System (GPS) “Electronic Stake Out” (ESO) devices were deployed on “bait” bicycles eighty-five (85) times during this reporting period, resulting in forty-nine (49) arrests.</p> <p>GPS “Slap-N-Track” (SNT) devices were used in two investigations during this reporting period: (1) a robbery and laptop snatch series involving multiple cases and suspects in Berkeley and in the region, with all suspects ultimately arrested; and (2) a currently-active case involving a series of auto burglaries in Berkeley and in the region.</p> <p>Data may be shared with the District Attorney’s Office for use as evidence to aid in prosecution, in accordance with laws governing evidence; other law enforcement personnel as a part of an active criminal investigations; and other third parties, pursuant to a court order.</p>
Geographic Deployment	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>GPS ESO-equipped bikes were deployed primarily in commercial districts across the city where bikes are frequently stolen.</p> <p>GPS SNT devices are deployed with judicial pre-approval, based on suspect location, rather than geographical consideration.</p>
Complaints	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There were no complaints made regarding GPS Trackers.</p>
Audits and Violations	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p> <p>There were no audits and no known violations relating to GPS Trackers.</p>
Data Breaches	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There were no known data breaches relating to GPS Trackers.</p>

<p>Effectiveness</p>	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>GPS Trackers continue to be very effective in apprehending bicycle thieves, many of whom are repeat offenders who've committed not only bike thefts, but other crimes as well. SNT trackers are effective in that they provide invaluable information on suspect vehicle location during the investigation of complex cases where suspects may be moving around the Bay Area and beyond.</p> <p>GPS Trackers greatly reduce costs associated with surveillance operations. A bike may be left for days. Surveillance operations generally involve four or more officers for the entire duration of an operation. A moving surveillance is extremely resource-intensive, requiring multiple officers in multiple vehicles for extended periods of time. Using both types of GPS trackers eliminates the need for officers' immediate presence until officers are ready to apprehend the suspect(s).</p>
<p>Costs</p>	<p>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</p> <p>The annual cost for the GPS Trackers' data service is \$1,920; the total cost for the 19 month period of this initial report was \$3,040. Further information regarding costs is contained in Policy 1301a, the Surveillance Acquisition Report.</p> <p>There are staff time costs associated with preparing and placing SNT trackers. The investigator must prepare a search warrant and obtain a judge's approval, and a small number of officers must place the tracker on the suspect's car. The total number of hours is a fraction of the time it would take to do a full surveillance operation involving numerous officers.</p> <p>There are staff time costs associated with preparing ESO trackers and placing ESO tracker-equipped bikes for bait bike operations. These are on the order of two-four hours per operation. The total number of hours is extremely small, given the large number of operations, and resulting arrests.</p>

## Surveillance Use Policy - GPS Tracking Devices

### 1301.1 PURPOSE

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals. GPS trackers electronically relay their precise location in real time, and thereby assist BPD in the recovery of evidence and arrest of suspects.

### 1301.2 AUTHORIZED USE

GPS trackers shall only be used during active criminal investigations. GPS trackers shall only be used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

GPS trackers shall only be utilized for law enforcement purposes.

### 1301.3 DATA COLLECTION

Location data may be obtained through the use of a GPS Tracker.

### 1301.4 DATA ACCESS

Access to GPS tracker data shall be limited to Berkeley Police Department (BPD) personnel utilizing the GPS Tracker(s) for active criminal investigations. Information may be shared in accordance with 1301.9 below.

In support of active criminal investigations, BPD personnel may receive GPS tracker data from probation or parole agencies which utilize GPS trackers (e.g. ankle monitors) as a condition of probation or parole.

### 1301.5 DATA PROTECTION

The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access.

### 1301.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1301.4 Data Access, 1301.5 Data Protection, 1301.7 Data Retention, 1301.8 Public Access and 1301.9 Third Party Data Sharing serve to protect against any unauthorized use of GPS tracker data. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### 1301.7 DATA RETENTION

A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker

identification label. This data is stored indefinitely by the vendor. The data does not contain any images, names of subjects, vehicle information, etc.

Tracker data received from the vendor shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant.

**1301.8 PUBLIC ACCESS**

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

**1301.9 THIRD-PARTY DATA-SHARING**

Data collected from the GPS trackers may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;
- (c) Other third parties, pursuant to a Court Order.

**1301.10 TRAINING**

Training for the operation of the GPS trackers shall be provided by BPD personnel. All BPD personnel shall be provided with this Surveillance Use Policy.

**1301.11 AUDITING AND OVERSIGHT**

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

**1301.12 MAINTENANCE**

GPS trackers shall only be obtained with the permission of the Investigations Division Captain or his/her designee. The Investigations Division Captain or his/her designee will ensure the trackers are returned when the mission/investigation is completed.

1301 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - GPS TRACKING DEVICES

---

**GPS TRACKING DEVICES**

**A. DESCRIPTION**

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals.

The Berkeley Police Department currently uses two types of GPS Tracking Devices to track the movements of vehicles, bicycles, or other kinds of property. The manufacturer, 3SI Security Systems, describes them as follows:

1. The "Slap-n-Track" (SNT) tracker tracks vehicles, cargo, and other large assets for long deployments. Offers extended battery life, rugged and weatherproof housing, and optional magnets.
2. The "Electronic Stake Out" (ESO) tracker offers Law Enforcement miniaturized and covertly packaged GPS Tracking Solutions to target property crimes, especially pattern crimes, in their local jurisdictions.

**B. PURPOSE**

Global Positioning System (GPS) tracking devices provide precise, real-time location information during the conduct of active criminal investigations. GPS trackers are only used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

**C. LOCATION**

GPS tracking devices shall be deployed in locations consistent with the authority granted by consent or a lawfully issued search warrant or court order.

**D. IMPACT**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. GPS Trackers are used in place of expensive, resource-intensive surveillance operations which typically involve multiple officers, often over long periods of time. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with GPS trackers help to ensure no unauthorized use of of GPS tracker data occurs. BPD Policy 1301 Surveillance Use Policy – GPS Tracking Devices ensure the use of GPS trackers and the resulting data are not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

**1301 APPENDIX A**

**BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - GPS TRACKING DEVICES**

---

**E. MITIGATION**

Data from a GPS tracker is encrypted from the vendor. Data shall be maintained in a secure, non-public location, such as locations requiring security access or badge access, thereby safeguarding the public from any impacts identified in subsection (D).

**F. DATA TYPES AND SOURCES**

A GPS tracker data record consists of date, time, latitude, longitude, map address (derived by using latitude, longitude and Google maps), and tracker identification label. The data does not contain any images, names of subjects, vehicle information, etc.

**G. DATA SECURITY**

Data from a GPS tracker is encrypted by the vendor on secure servers. The data is only accessible through a secure website to BPD personnel who have been granted security access. Captains whose Divisions utilize GPS trackers are responsible for ensuring compliance with the procedures for utilizing GPS Trackers.

**H. FISCAL COST**

The initial cost of the GPS trackers totaled \$4,335.

- Between 2015-present BPD purchased 5 GPS "ESO" trackers for \$2,250 (\$450 each).
- In 2017 BPD purchased 3 GPS "SNT" trackers for \$2,085 (\$695 each).

The annual cost for the GPS data service totals \$1,920.

- The annual data service for the five ESO trackers is \$1,020 (\$204 each).
- The annual data service for the three SNT trackers is \$900 (\$300 each).

Personnel costs are minimal in that the GPS trackers are used as a resource during normal working hours.

GPS trackers are funded through the Investigations Division's general budget.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

Data collected from the GPS trackers may be shared with the following:

- a. The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- b. Other law enforcement offices as part of a criminal investigation;
- c. Other third parties, pursuant to a Court Order.

**1301 APPENDIX A**

**BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - GPS TRACKING DEVICES**

---

**J. ALTERNATIVES**

An alternative to the use of GPS trackers is to conduct resource-intensive surveillance operations utilizing numerous personnel over extended periods of time.

**K. EXPERIENCE OF OTHER ENTITIES**

The use of GPS tracker technology is common amongst law enforcement agencies throughout the country.



**ATTACHMENT 4:**  
**Automated License Plate Readers**

**Surveillance Technology Report: Automated License Plate Readers**

**March 1, 2018 – Sept. 30, 2019**

<p>Description</p>	<p>A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing.</p> <p>Automated License Plate Readers (ALPRs) are used by Parking Enforcement Bureau vehicles for time zone parking and scofflaw enforcement. The City’s Transportation Division uses anonymized information for purposes of supporting the City’s GoBerkeley parking management program. ALPR use replaced the practice of physically “chalking” tires.</p> <p style="text-align: center;"><b>Summary of ALPR Time Zone Enforcement Data</b></p> <p style="text-align: center;">Read Data</p> <p style="text-align: center;">There were an average of 9,075 “Reads” per working day (Based on one month’s data: 9/9/19-10/9/19)</p> <p style="text-align: center;">Hit Data</p> <p style="text-align: center;">There were 69,738 “Hits” 18,410 “Enforced Hits” resulted in citation issuance. 51,328 “Not Enforced” Hits resulted in no citation issuance. (Based on one year’s data: 10/9/18-10/9/19)</p> <p>Genetec is the vendor for the ALPR Time Zone enforcement system. A “read” indicates the ALPR system successfully read a license plate. A “hit” indicates the ALPR system detected a possible violation, which prompts the Parking Enforcement Officer to further assess the vehicle. In many cases, hits are “rejected” or “not enforced” because the Parking Enforcement Officer determines the vehicle has an appropriate placard or permit, or there is other information which precludes citation.</p> <p style="text-align: center;"><b>Summary of ALPR Booting Scofflaw Enforcement Data</b></p> <p style="text-align: center;">255 vehicles booted from 9/1/18-6/30/19</p> <p>Paylock is the vendor for the ALPR Booting Scofflaw Enforcement Program. A single parking enforcement vehicle is equipped with the Paylock system ALPR. The Paylock ALPR system provides the operator a “hit” when a plate is recognized as having five or more unpaid parking tickets. The operator then further assesses the vehicle, confirms the citation data, and, if confirmed, creates a boot entry in Paylock, and boots the car.</p> <p>Paylock uploads and retains information to their secure server solely on <i>confirmed</i> boots or tows. Hits and reads are not retained in the Paylock server. Booting Scofflaw enforcement has been temporarily suspended due to the transition to a different citation management vendor.</p>
--------------------	--

	<p>All BPD ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes, or as otherwise permitted by law. All ALPR data is subject to the provisions of BPD Policy 415 - Immigration Law, and therefore may not be shared with federal immigration enforcement officials.</p>
Geographic Deployment	<p>Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically.</p> <p>Only Parking Enforcement Vehicles are equipped with ALPRs. ALPRs are deployed based on areas where there are parking time restrictions. ALPRs are not deployed based on geographic considerations not related to parking and scofflaw enforcement.</p>
Complaints	<p>A summary of each complaint, if any, received by the City about the Surveillance Technology.</p> <p>There have been no complaints about the deployment and use of Automated License Plate Readers.</p>
Audits and Violations	<p>The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response.</p> <p>There have been no complaints of violations of the ALPR Surveillance Use Policy.</p>
Data Breaches	<p>Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.</p> <p>There have been no known data breaches or other unauthorized access to Automated License Plate Reader data.</p>
Effectiveness	<p>Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes.</p> <p>ALPRs have proven effective in parking enforcement for time zone enforcement.</p> <p>ALPRs have proven effective in supporting enforcement upon vehicles which have five or more unpaid citations. The ALPR's ability to read and check license plates while being driven greatly increases efficiency, allowing an operator to cover larger areas more quickly without having to stop except to confirm a hit.</p>
Costs	<p>Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.</p> <p>The annual system maintenance cost for Genetec is \$47,000. This cost is borne by the Transportation Division, which also purchased the ALPR units used in Time Zone Enforcement.</p> <p>No Genetec LPR units were purchased during the period covered by this report.</p> <p>Genetec ALPR units are in use on 20 Parking Enforcement vehicles. Parking Enforcement personnel perform a variety of parking enforcement activities, and are not limited solely to time zone enforcement. Therefore, personnel costs specifically attributable to time zone enforcement are not tracked.</p>

The cost of Paylock is \$140 per boot.

One Parking Enforcement Officer is assigned to scofflaw enforcement and abandoned auto enforcement on a full time basis. Assuming the Officer works approximately half their day on scofflaw enforcement, the annual personnel cost would be approximately one half a fulltime Parking Enforcement Officer's pay with benefits, or \$65,000.

## Surveillance Use Policy - ALPR

### 1302.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by BMC 2.99.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. (Ref. policy 422.2)

### 1302.2 AUTHORIZED AND PROHIBITED USES USE

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53). (Ref. policy 422.4)

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used to support a patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

### 1302.3 DATA COLLECTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law. (Ref. policy 422.5)

### 1302.4 DATA ACCESS

- (a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (c) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

---

### **1302.5 DATA PROTECTION**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.6):

- (a) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- (c) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (d) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

### **1302.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### **1302.7 DATA RETENTION**

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT) department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)

- (a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

### **1302.8 PUBLIC ACCESS**

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. (Ref. policy 422.6 (a))
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question. (Ref. policy 422.6 (b))

### **1302.9 THIRD-PARTY DATA-SHARING**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. ALPR data is subject to the provisions of BPD Policy 415, and hence may not be shared with federal immigration enforcement officials.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager. (Ref. policy 422.6 (e))

### **1302.10 TRAINING**

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

### **1302.11 AUDITING AND OVERSIGHT**

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. (Ref. policy 422.6 (g))

### **1302.12 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. (Ref. policy 422.3)

#### **1302.12.1 ALPR ADMINISTRATOR**

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref.

policy 422.3.1):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.



## AUTOMATED LICENSE PLATE READER (ALPR) DEVICES

### A. DESCRIPTION

Automated License Plate Readers (ALPRs) are high-speed, computer controlled camera systems that are typically mounted on Berkeley Police Department Parking Enforcement Vehicles.

ALPRs capture license plate numbers which come into view, along with the location, date and time. The data, which includes a photo of the front or the back of the car displaying the license plate, is then uploaded to a central server.

### B. PURPOSE

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the California Law Enforcement Telecommunications System's (CLETS) Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

### C. LOCATION

Parking Enforcement vehicles travel throughout the city; using the ALPRs as described above.

### D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with ALPR Units will help to ensure unauthorized use of its data. The procedures will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1302 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES

---

**E. MITIGATION**

All saved data will be safeguarded and protected by both procedural and technological means which are implemented to safeguard the public from any impacts identified in subsection (D). See subsection (G) for further.

**F. DATA TYPES AND SOURCES**

Photographs of license plates and location data may be obtained through the use of ALPR Units.

**G. DATA SECURITY**

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
2. Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
3. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
4. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

**H. FISCAL COST**

In 2015, Public Works brought an ALPR Contract to City Council. Council approved a contract for Public Works to buy five Genetec ALPR Units with PCS Mobile communication, for a pilot program for \$450,000.

In 2017, after success with the program, City Council approved an amendment to the contract, allowing Public Works to purchase 15 more ALPR Units for Parking Enforcement vehicles, and to continue its use of PCS Mobile, for 1,200,000. The money was allocated from the goBerkeley/Federal Highway Administration Parking Meter Fund.

Yearly service for the ALPR Units includes warranties, hosting services, cellular connection, mobile computing, and training which varies. The costs through fiscal year 2022 are currently estimated at \$1,175,000.

## 1302 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES

---

Personnel costs are minimal in that the ALPR Units are used as a resource during normal working hours.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

1. Vendor Access-Scofflaw Enforcement: The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:
  - a. All data captured by the ALPR is stored on the booting vehicle's laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.
  - b. When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.
2. Vendor Access-General Parking Enforcement and goBerkeley Program: The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.
  - a. In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.
  - b. The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.
3. Department of Information Technology Access: Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who

## 1302 APPENDIX A

**BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES**

---

do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

4. Other Law Enforcement Agency Access: ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55). Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
5. Member Access: No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training. No ALPR operator may access CLETS data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.
6. Public Access: Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

**J. ALTERNATIVES**

None.

**K. EXPERIENCE OF OTHER ENTITIES**

The use of ALPR technology is common amongst law enforcement agencies throughout the country, in support of parking enforcement, and law enforcement criminal investigations.

---

## Automated License Plate Readers (ALPRs)

### 422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

### 422.3 ADMINISTRATION

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

#### 422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### 422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use,

---

or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.
- (b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert

#### **422.5 .DATA COLLECTION AND RETENTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review.

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT Department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

- (a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.
- (b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not

---

showing violations will not be transferred to the server.

#### **422.6 ACCOUNTABILITY**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

For security or data breaches, see the Records Release and Maintenance Policy.

#### **422.7 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  - 1. The name of the agency.
  - 2. The name of the person requesting.
  - 3. The intended purpose of obtaining the information.

- 
4. The related case number.
  - (b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.
  - (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

#### **422.8 SCOFFLAW ENFORCEMENT**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

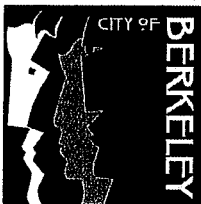
The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking



enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

**ATTACHMENT 5:**  
**Police Review Commission Communication**



Police Review Commission (PRC)

September 11, 2019

To: Honorable Mayor and Members of the City Council  
From: George Perezvelez, <sup>PRC 0449</sup> Chairperson, Police Review Commission  
Re: Proposed Berkeley Police Department Policy 422, Automated License Plate Readers

Summary: This memo is to inform you of the Police Review Commission's qualified approval of the BPD's proposed policy for the use of Automated License Plate Readers (ALPRs).

Background: The BPD submitted the ALPR policy, Policy 422, to the PRC for review, along with the Surveillance Use Policy and the Surveillance Acquisition Report (Policy 1302 and Appendix A) for these devices. This process was undertaken in advance of BPD submitting these items to the City Council as required by the Surveillance Technology Use and Community Safety Ordinance (B.M.C. Ch. 2.99).

These policies were first considered by the full Commission, which then referred them to its Lexipol Policies Subcommittee. In response to feedback from the PRC and the Subcommittee, the BPD revised the proposed policy, which was reviewed by both bodies. At various stages, the PRC and the subcommittee had the opportunity to hear from and ask questions of Police Chief Greenwood and other members of the BPD, and Deputy City Attorney Chris Jensen. The PRC also heard input from representatives of Media Alliance and Oakland Privacy.

Final action: At its September 4, 2019 meeting, the PRC voted to approve for submission to the City Council for your review and discussion the version of Policy 422 that is attached here, with two caveats. First, there was concern among some commissioners that the ALPR was originally acquired for the purpose of parking enforcement and that this policy represents an expansion of that function. If this is not what the Council had in mind, then this policy should be modified accordingly. Second, Section 422.4(c) of the policy does not adequately define what constitutes a "crime scene."

Finally, the Commission wishes to remind the Council that they will see actual use of the ALPR technology under the reporting mechanism in place in the Surveillance Technology Use and Community Safety Ordinance.

Honorable Mayor and Members of the City Council  
Proposed Berkeley Police Department Policy 422, Automated License Plate Readers  
September 11, 2019  
p. 2

The above action was approved by the following vote: Moved/Seconded  
(Perezvelez/Mikiten) -- Ayes: Calavita, Chang, Leftwich, Mikiten, Perezvelez,  
Ramsey; Noes: Earnest, Mizell; Abstain: Allamby; Absent: None.

Attachment: Revised Policy 422

cc: Dee Williams-Ridley, City Manager  
Andrew Greenwood, Chief of Police  
David White, Deputy City Manager  
PRC Commissioners

---

## Automated License Plate Readers (ALPRs)

### 422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

### 422.3 ADMINISTRATION

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

#### 422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### 422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use,

---

or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.
- (b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

#### **422.5 DATA COLLECTION AND RETENTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ~~ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.~~

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT Department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

- (a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.

- 
- (b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not showing violations will not be transferred to the server.

#### **422.6 ACCOUNTABILITY**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

For security or data breaches, see the Records Release and Maintenance Policy.

#### **422.7 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  1. The name of the agency.

- 
2. The name of the person requesting.
  3. The intended purpose of obtaining the information.
  4. The related case number.
- (b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

#### **422.8 SCOFFLAW ENFORCEMENT**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

- (a) All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated



with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.



Office of the City Manager

ACTION CALENDAR  
September 13, 2022  
(Continued from July 26, 2022)

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Andrew Greenwood, Chief of Police  
David White, Deputy City Manager

Subject: Surveillance Technology Report, Surveillance Acquisition Report, and  
Surveillance Use Policy for Automatic License Plate Readers

RECOMMENDATION

Adopt a Resolution accepting the Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers submitted pursuant to Chapter 2.99 of the Berkeley Municipal Code.

FISCAL IMPACTS OF RECOMMENDATION

There are no fiscal impacts associated with adopting the attached resolution.

CURRENT SITUATION AND ITS EFFECTS

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”). The purpose of the Ordinance is to provide transparency surrounding the use of surveillance technology, as defined by Section 2.99.020 in the Ordinance, and to ensure that decisions surrounding the acquisition and use of surveillance technology consider the impacts that such technology may have on civil rights and civil liberties. Further, the Ordinance requires that the City evaluate all costs associated with the acquisition of surveillance technology and regularly report on their use.

The Ordinance imposes various reporting requirements on the City Manager and staff. The purpose of this staff report and attached resolution is to satisfy annual reporting requirements as outlined in sections 2.99.050 and 2.99.070. The attached Surveillance Technology Reports, Surveillance Acquisition Reports and Surveillance Use Policies for Automatic License Plate Readers, GPS Trackers, and Body Worn Cameras are for technologies that were acquired by the City prior to the adoption of the Ordinance.

Section 2.99.050 of the Ordinance required the City Manager to submit a Surveillance Acquisition Report and Surveillance Use Policy for each surveillance technology that has been possessed or used prior to the effective date of the Ordinance. The requirements of this section were not satisfied due to a multitude of factors, and the Police Department opted to submit the attached acquisition reports and use policies to the Police Review Commission prior to their review by the City Council. The Police Review Commission underwent an extensive engagement process and the full Commission discussed the attached use policies and reports at scheduled meetings from May to October 2019. In all cases, the Police Review Commission approved the attached acquisition reports and use policies and conveyed any concerns or suggested modifications to the Police Chief. In addition to the technologies covered by the attached resolution, City staff continues to evaluate whether or not there is any other technology that is used or possessed that is subject to the Ordinance.

Finally, Section 2.99.040 of the Ordinance allows the City Manager to borrow, acquire, or temporarily use surveillance technology in exigent circumstances without having to obtain the approval of City Council. Since the adoption of the ordinance, the City is reporting two instances in which the City Manager has made use of Section 2.99.040. In preparation for the potentially violent August 5, 2018 demonstration in downtown Berkeley, the City borrowed remote accessible cameras from the Northern California Regional Intelligence Center (NCRIC) in order to have the ability to remotely monitor intersections in real time. The cameras did not have face recognition technology. Signage was posted in the areas of the cameras, informing people that the area may be under video surveillance. Using cameras to monitor intersections is at times preferable to physically placing officers in those locations. In addition, as a mutual aid resource, the Police Department requested the Alameda County Sheriff's Office Small Unmanned Aerial System (sUAS) team as a mutual aid resource. The purpose of the request was to support the identification and apprehension of any felony suspects, should a felony occur. Following the felony vandalism of over ten City of Berkeley vehicles, the sUAS team deployed a drone, but no suspects were apprehended.

## BACKGROUND

On March 27, 2018, the City Council adopted Ordinance 7,592-N.S., adding Chapter 2.99 to the Berkeley Municipal Code, which is also known as the Surveillance Technology Use and Community Safety Ordinance. The Ordinance contains various reporting requirements including the following:

- Section 2.99.050, which requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the Ordinance; and

- Section 2.99.070 of the Ordinance, which requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November.

For each of the three technologies, the Surveillance Technology Report, Surveillance Acquisition Report and Surveillance Use Policies were prepared to satisfy the specific, section-by-section requirements of the Ordinance, and are attached to this report. It should be noted that substantial policies already existed for Body Worn Cameras and License Plate Readers. Those policies—also reviewed by the Police Review Commission for purposes of this report—are also attached. The existing policies will continue to remain in effect upon Council’s approval. Henceforth, all new Surveillance Use Policies and Surveillance Acquisition Reports will be listed in Chapter 13 of the Berkeley Police Department Policy Manual, which is being created to provide easy access to all policies relating to BMC 2.99. All BPD policies are available to the public on BPD’s website.

ENVIRONMENTAL SUSTAINABILITY

There are no identifiable environmental effects or opportunities associated with the content of this report.

RATIONALE FOR RECOMMENDATION

City Council is being asked to adopt the attached resolution for the City to be in compliance with the Ordinance.

ALTERNATIVE ACTIONS CONSIDERED

City Council could decide not to adopt the resolution or could direct staff to revise the attached policies.

CONTACT PERSON

Andrew Greenwood, Chief of Police, (510) 981-7017  
David White, Deputy City Manager, (510) 981-7012

ATTACHMENTS

1. Proposed Resolution

2. Body Worn Cameras

Surveillance Technology Report: Body Worn Cameras

Policy 1300 Body Worn Camera Use Policy

Policy 1300(a) Appendix: Body Worn Camera Acquisition Report

Policy 425 Body Worn Camera Policy (Existing Policy)

3. Global Positioning System Tracking Devices

Surveillance Technology Report

Policy 1301 Global Positioning System Tracking Devices Use Policy

Policy 1301(a) Appendix: Global Positioning System Tracking Devices Acquisition Report

4. Automated License Plate Readers

Surveillance Technology Report: Automated License Plate Readers

Policy 1302 Automated License Plate Reader Use Policy

Policy 1302(a) Appendix: Automated License Plate Reader Acquisition Report

Policy 422 Automated License Plate Reader (Latest version of existing Policy)

5. Police Review Commission Memorandum Regarding Automatic License Plate Readers

i:\surveillance ordinance\city council meeting -- 11-12-19\11-12-2019\_surveillance ordinance staff report and resolution (04).docx

RESOLUTION NO. ##,###-N.S.

A RESOLUTION ACCEPTING THE SURVEILLANCE TECHNOLOGY REPORT, SURVEILLANCE ACQUISITION REPORT, AND SURVEILLANCE USE POLICY FOR AUTOMATIC LICENSE PLATE READERS

WHEREAS, on March 27, 2018, the City Council adopted Ordinance 7,592-N.S., which is known as the Surveillance Technology Use and Community Safety Ordinance (“Ordinance”); and

WHEREAS, Section 2.99.050 of the Ordinance requires that the City Manager shall submit a Surveillance Acquisition Report and a proposed Surveillance Use Policy for each piece of technology governed by the Ordinance that had been possessed or used by the City prior to the effective date of the Ordinance; and

WHEREAS, Section 2.99.070 of the Ordinance requires that the City Manager must submit to the City Council a Surveillance Technology Report as defined by Section 2.99.020(2) of the Ordinance at the first regular City Council meeting in November; and

WHEREAS, the Surveillance Acquisition Report and Surveillance Use Policy for Automatic License Plate Readers satisfies the requirements of the Ordinance.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley:

Section 1. Pursuant to Section 2.99.060, as it pertains to the use of Automatic License Plater Readers, the City Council hereby finds and determines the following:

- a. The benefits of using the technology outweighs the costs;
- b. The policies attached to this resolution safeguard civil liberties; and
- c. No feasible alternatives exist with similar utility that will have a lesser impact on civil rights or liberties.

Section 2. The City Council hereby accepts the Surveillance Technology Report, Surveillance Acquisition Report, and Surveillance Use Policy for Automatic License Plate Readers.

ATTACHMENT 2:  
BODY WORN CAMERAS

Surveillance Technology Report Body Worn Cameras  
To be provided as part of supplemental communications



---

## Surveillance Use Policy - Body Worn Cameras

### 1300.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department Body Worn Camera Policy #425 and adds elements as required by BMC 2.99.

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel. (Ref. policy 425.2)

### 1300.2 AUTHORIZED USE

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The BWC shall be activated in any of the following situations:

- (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- (c) Self-initiated field contacts in which a member would normally notify the Communications Center.
- (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
- (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

---

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation. (Ref. policy 425.7)

#### 1300.2.1 PROHIBITED USE

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule. (Ref. policy 425.13)

#### 1300.3 DATA COLLECTION

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. (Ref. policy 425.3)

#### 1300.4 DATA ACCESS

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 1300.4.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report. (Ref. policy 425.17)

##### 1300.4.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH

- (a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed the video files.

- It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.
- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
  - (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
  - (d) Prior to the conclusion of the criminal interview process, the involved member and/ or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.
  - (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident." (Ref. policy 425.17.1)

#### 1300.4.2 SUPERVISORY REVIEW

With the exception of section 1300.4.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates. (Ref. policy 425.17.2)

#### 1300.4.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance. (Ref. policy 425.17.3)

- (a) Recorded files may also be reviewed:
  1. Upon approval by a supervisor, by any member of the Department who is participating

in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.

2. Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
  3. By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
  4. Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.
- (b) Investigators conducting criminal or internal investigations shall:
1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
  2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
  3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

#### 1300.4.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video. (Ref. policy 425.17.4)

#### 1300.4.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee. (Ref. policy 425.17.5)

### 1300.5 DATA PROTECTION

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. (Ref. policy 425.14)

### **1300.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of BWC data. These policies will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### **1300.7 DATA RETENTION**

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days. (Ref. policy 425.15)

### **1300.8 PUBLIC ACCESS**

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy. (Ref. policy 425.18)

### **1300.9 THIRD-PARTY DATA-SHARING**

#### **1300.9.1 CITY ATTORNEY**

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

---

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur. (Ref. policy 425.18)

#### 1300.9.2 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation. (Ref. policy 425.18.1)

- (a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

#### 1300.10 TRAINING

Training for the operation of BWC's shall be provided by BPD personnel. All BPD personnel who use BWC's shall be provided a copy of this Surveillance Use Policy.

#### 1300.11 AUDITING AND OVERSIGHT

Division Captains for divisions utilizing BWC's shall ensure compliance with this Surveillance Use Policy.

#### 1300.12 MAINTENANCE

The BWC system will be maintained by the Applications Programmer Analyst and assigned

Department of Information and Technology (IT) staff.

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18) (Ref policy 425.4):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.
- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.
- (h) All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

## 1300 APPENDIX A

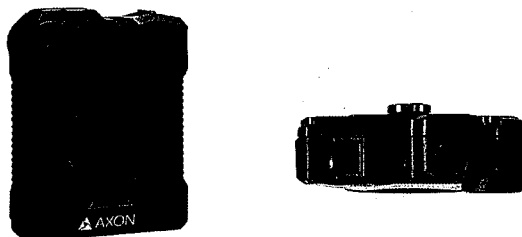
BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS

---

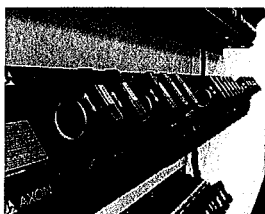
**BODY WORN CAMERAS (BWCs)****A. DESCRIPTION**

The BWC system consists of four main components: The camera, the docking station, and the Digital Information Management System (DIMS) and smartphone applications.

The first component, the Axon camera, is a system which incorporates an audio and video recording device. It is designed to record events in real time for secure storage, retrieval, and analysis. The camera is to be attached to an officer's uniform and is powered by an internal rechargeable battery. The camera features low-light performance, full-shift battery life, a capture rate of 30 frames per second with no dropped frames, HD video, pre-event buffering, multi-camera playback, and the ability to automatically categorize video using the police department's computer aided dispatch system. An officer can start and stop recording by pressing a button on the front of the camera. The camera does not contain a screen for footage review.



The second component of the system is the docking station. Once the Axon camera is placed in the docking station it recharges the camera's battery. The dock also triggers the uploading of data from the camera to a cloud based Digital Information Management System (DIMS) called Evidence.com. The dock does not directly provide functionality to view, modify or delete video data stored on Axon cameras.



The third component is the Digital Information Management System called Evidence.com. Evidence.com streamlines data management and sharing on one secure platform. The evidence management system is comprehensive, secure, and intuitive to use. The DIMS is located in a cloud-based data center for security, scalability, and ease of administration. Users can add



**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

metadata to existing videos such as associated case numbers, incident type, incident dispositions, etc. to make the videos easier to find. However, the videos themselves cannot be altered by the user.

The fourth component of the system to be utilized are two Axon mobile applications, which allow officers to collect and review evidence in the field and more effectively use their BWCs. The applications use secure Bluetooth and Wi-Fi technology to access the BWC systems and footage. These applications are compliant with US Department of Justice evidentiary standards, meaning that they are both secure and are set up in a way that prohibits the altering or destruction of evidence. The applications are called Axon View and Axon Capture. Axon View allows users to change their camera settings, view live video, and review and tag recorded videos while they are stored on the BWC. Recorded videos remain in the BWC's memory, and cannot be manipulated or deleted. Axon Capture allows officers to use their city-issued smartphone's camera and microphone to take photographs, and record audio and video, and to upload this data directly to Evidence.com. These applications do not allow users to alter, manipulate, or edit any of the footage recorded by the BWC. These applications use secure technology to add value and efficiency to the BWC program.

**B. PURPOSE**

The primary objective of the BWC system is to document officer contacts, arrests, and critical incidents. Video footage collected by the BWCs will be used as evidence in both criminal and administrative investigations. Video footage not relevant to any investigation will be discarded after a defined retention period.

In instances where the officer might be expected to take law enforcement action of any kind, the officer is expected to record the encounter for the benefit of both the officer and the member of the public.

1. The BWC shall be activated in any of the following situations:
  - i. All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
  - ii. Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
  - iii. Self-initiated field contacts in which a member would normally notify the Communications Center.
  - iv. Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

- v. Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- vi. Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is an officer expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the user can do so safely.

Officers should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Officers shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

2. Prohibited uses of the BWC system include:

- i. Officers shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.
- ii. Officers are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.
- iii. Officers are prohibited from retaining BWC recordings.
- iv. Officers shall not duplicate or distribute such recordings, except for department business purposes.

**C. LOCATION**

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers, in accordance with BPD policy #425.

**D. IMPACT**

With the introduction of BWCs, officers record all enforcement contacts with the public. To that end, an officer could find themselves engaged in their lawful duties in both public and private areas. Additionally, due to the nature of law enforcement work, an officer may be required to engage in sensitive conversations with individuals of all ages, including children.

The right to maintain someone's anonymity versus the need to gain information to maintain public safety is of paramount concern. The Department recognizes that all people have a right to privacy and is committed to protecting and safeguarding civil rights by adhering to the

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

strictest requirements of both state and federal law concerning release of audio/video recordings.

**E. MITIGATION**

In order to minimize violations of privacy, BWC policy provides that:

1. Officers should record any incident they feel would be appropriate or valuable to document. The BWC policy shall require officers to activate the BWC under the criteria listed above.
2. Officers should not activate the BWC and/or use caution when entering a public locker room, changing room, restroom, doctor's or attorney's office, or other place where individuals unrelated to the investigation are present and would have a heightened expectation of privacy unless the officer is investigating criminal activity or responding to a call for service.
3. BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy.
4. BWC footage will be retained or released in accordance with applicable state and federal law. Criminal defendants will have access to relevant BWC footage via the court discovery process.
5. Officers are prohibited from retaining BWC recordings, Officers shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.
6. Officers are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Officers may request restriction and subsequent deletion of an accidental recording according to the BWC policy.
7. Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted by law and department policy. Department policy does not authorize release of investigative files or documents that would constitute an unwarranted invasions of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy"

**F. DATA TYPES AND SOURCES**

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigations, and other proceedings protected by confidentiality laws and department policy.

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

The BWC collects video and audio recordings of events occurring in the user's presence. As each video is created, the system automatically stamps the video with the current date/time and the camera user's identity. The user has the option to add metadata manually to existing recordings after they are created. Such metadata may include but is not limited to:

1. Category of contact (from Department's defined list)
2. Disposition of contact (arrest, citation, etc.)
3. Associated case number

**G. DATA SECURITY**

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for transferring the data into the digital evidence management system. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings.

Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited. The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code Section 832.18) (Ref. policy 425.14):

1. Establishing a system for uploading, storing and security of recordings.
2. Designating persons responsible for uploading recorded data.
3. Establishing a maintenance system to ensure availability of BWCs.
4. Establishing a system for tagging and categorizing data according to the type of incident captured.
5. Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
6. Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
7. Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file,

**1300 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS**

---

thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

**H. FISCAL COST**

In 2017, the Berkeley City Council approved a resolution authorizing a contract between BPD and Axon. Axon was chosen after a competitive Request for Proposal (RFP) process. The contract will not exceed \$1,218,103 and includes the cost of 200 body worn cameras, charging stations, accessories, software licenses, training and unlimited storage for five years. The purchase also includes replacement cameras and charging stations during the third and fifth year of the contract.

There will be an annual cost of approximately \$250,000 to the police department's budget for a staff person to administer the body worn camera program beginning in FY 2019.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

All BWC data will be uploaded and stored on Axon Cloud Services, Evidence.com. Axon complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States (collectively, "Privacy Shield"). Axon has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

**J. ALTERNATIVES**

Officers rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras and/or not utilizing BWCs. However, BPD sees the use of BWCs as an integral strategy to strengthen police transparency, prevent and resolve complaints against the police by civilians, document police-public interaction, and promote the perceived legitimacy and sense of procedural justice that communities have about their departments. There is a broad consensus – among community leaders, the ACLU, the Department of Justice, the Berkeley Police Department, and elected officials – that body-worn cameras can be an important tool for improving the high-quality public service expected of police officers.

1300 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - BODY WORN CAMERAS

---

**K. EXPERIENCE OF OTHER ENTITIES**

Numerous police agencies have adopted BWCs as a tool to help combat crime, to reduce citizen complaints and to reduce use of force situations. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration, [https://www.bja.gov/bwc/pdfs/14-005\\_Report\\_BODY\\_WORN\\_CAMERAS.pdf](https://www.bja.gov/bwc/pdfs/14-005_Report_BODY_WORN_CAMERAS.pdf) - pages 6-8, cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard, <https://www.bwccscorecard.org/>, provides an analysis of how scores of different police agencies have employed BWCs through a defined list of metrics.

---

## Body Worn Cameras

### 425.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable Body Worn Cameras (BWCs) by members of this department while in the performance of their duties.

This policy does not apply to non-BWC evidence, including other methods of audio or video recordings, interviews or interrogations conducted at any Berkeley Police Department facility, authorized undercover operations, wiretaps or eavesdropping (concealed listening devices).

### 425.2 POLICY

The Berkeley Police Department recognizes that video recording of contacts between department personnel and the public provides an objective record of these events, and that the use of a recording system complements field personnel in the performance of their duties by providing a video record of enforcement and investigative field contacts, which can enhance criminal prosecutions, limit civil liability, increase transparency, and enhance professionalism in the delivery of police services to the community. A video recording of an event or contact also enables the delivery of timely, relevant, and appropriate training to maximize safety for both community members and BPD personnel.

While recordings obtained from BWCs provide an objective record of events, it is understood that video recordings do not necessarily capture all events, activities and information, or reflect the full experience of the individual member(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events as perceived and recalled by the involved member. Specifically, it is understood that the BWC will capture information that may not have been seen and/or heard by the involved member and that the involved member may see and hear information that may not have been captured by the BWC.

### 425.3 CONFIDENTIALITY AND PROPER USE OF RECORDINGS

BWC use is limited to enforcement and investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, training, civil litigation, and other proceedings protected by confidentiality laws and department policy. Improper use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded and is prohibited.

### 425.4 COORDINATOR

The Chief of Police, or his/her designee shall appoint a member of the Department to coordinate the use and maintenance of BWCs and the storage of recordings, including (Penal Code § 832.18):

- (a) Establishing a system for uploading, storing and security of recordings.
- (b) Designating persons responsible for uploading recorded data.

## Berkeley Police Department

Law Enforcement Services Manual

Body Worn Cameras

---

- (c) Establishing a maintenance system to ensure availability of BWCs.
- (d) Establishing a system for tagging and categorizing data according to the type of incident captured.
- (e) Establishing a system to prevent tampering, deleting and copying recordings and ensure chain of custody integrity.
- (f) Working with the City Attorney's office to ensure an appropriate retention schedule is being applied to recordings and associated documentation.
- (g) Maintaining an audit trail record for all access to evidence files, wherein access information for each evidence file is logged through use of a secure log-in system. The Department's storage system associates an audit trail record with each evidence file, thereby logging the date, time, user name, activity and client IP address occurring during each evidence file access.

All recordings made by members acting in their official capacity shall remain the property of the Department. Subject to the provisions of this Policy, members shall have no expectation of privacy or ownership interest in the content of these recordings.

**425.5 MEMBER RESPONSIBILITIES**

Prior to going into service, each uniformed member who is assigned to wear a BWC will be responsible for making sure that he or she is equipped with a BWC issued by the Department, and that the BWC is in good working order. If the BWC is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his/her supervisor to permit the supervisor or other department employee to provide the member with a functioning BWC as soon as practicable. Uniformed members should wear the recorder in a conspicuous manner as prescribed by the Department, to provide a generally unobstructed camera view of contacts between members of the public and department members.

Members lawfully engaged in their duties as a police officer are not required to obtain consent from, or give notice to, members of the public, prior to recording with their BWC.

Upon the approval of the Chief of Police, or his/her designee, non-uniformed members lawfully engaged in their duties as a police officer may use an approved BWC.

Members are required to document the existence of a recording in any report or other official record of the contact, such as a CAD entry, including any instance where the member is aware that the BWC malfunctioned or the member deactivated the recording. In the event activity outlined in section 425.7 is not captured in whole or in part the member shall document this and explain in their report their understanding, if any, of why the footage was not captured in the recording.

**425.6 SUPERVISOR RESPONSIBILITIES**

At such time as the scene is considered secure and safe, the on-scene supervisor shall take immediate physical custody of involved officer's/officers' BWC when the device may have captured an incident involving an officer-involved shooting or use of force resulting in death or great bodily injury, and shall ensure the data is uploaded in a timely manner as prescribed by BPD policy



## Berkeley Police Department

## Law Enforcement Services Manual

*Body Worn Cameras*

---

(Penal Code § 832.18). Supervisors may review relevant BWC video and audio files in the field in furtherance of their duties and responsibilities.

Supervisors shall also review relevant BWC recordings prior to submitting any administrative reports.

**425.7 ACTIVATION OF THE BODY WORN CAMERA**

This policy is not intended to describe every possible situation in which the BWC should be used. Members shall activate the BWC as required by this policy in (a)-(f) below, and may activate the BWC at any time the member believes it would be appropriate or valuable to record an incident within the limits of privacy described herein.

The BWC shall be activated in any of the following situations:

- (a) All in-person enforcement and investigative contacts including pedestrian stops and field interview (FI) situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- (c) Self-initiated field contacts in which a member would normally notify the Communications Center.
- (d) Any search activity, including the service of search or arrest warrants; probation, parole, or consent searches where the member is seeking evidence of an offense, or conducting a safety sweep or community caretaking sweep of the premises. Once a location has been secured and the member is not interacting with detainees or arrestees, the member may mute their BWC when conducting a search for evidence.
- (e) Any other contact that the member determines has become adversarial after the initial contact in a situation where the member would not otherwise activate BWC recording.
- (f) Transporting any detained or arrested person and where a member facilitates entry into or out of a vehicle, or any time the member expects to have physical contact with that person.

At no time is a member expected to jeopardize his or her safety in order to activate a BWC. The BWC should be activated by members in anticipation of situations described above, and in any unanticipated, rapidly unfolding situation where activation becomes required, as soon as the member can do so safely.

Members should activate their BWC when conducting custodial interviews unless there are other recording devices being used. Members shall document and explain in their report the reason for not recording custodial interviews, should a BWC be de-activated while conducting a custodial interview or interrogation.

## Berkeley Police Department

Law Enforcement Services Manual

Body Worn Cameras

---

**425.8 VICTIMS AND WITNESSES OF CRIMES; INFORMANTS**

In the event that an officer has the opportunity to record interviews of victims and witnesses of crimes, they shall consider the following:

- (a) **Witnesses:** In the event a crime witness or a member of the community wishes to report or discuss criminal activity anonymously, officers have the discretion to not record. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the witness's recorded statement. In cases where a witness requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
- (b) **Victims:** Upon request by the victim, officers have the discretion to not record the interview. Members may offer to avert their camera to capture only audio during the interview, when doing so would facilitate obtaining the victim's recorded statement. In cases where a victim requests they not be recorded, and the member agrees not to record, members should record their request prior to turning the camera off. When a member is already recording, the member shall record their explanation for turning the camera off prior to doing so.
  - 1. **Domestic Violence Victims:** Members should attempt to record interviews of domestic violence victims to facilitate future prosecution efforts and discourage later recanting of statements. Members should also record interviews with children who witness domestic violence, when the child is willing.
  - 2. **Child Abuse and Sexual Assault Victims:** Members shall have the discretion to record, absent any request to not record the interview by victims, witnesses, or non-suspect parents of victims, during child abuse and/or sexual assault investigations.
- (c) **Informants:** Members shall not activate their recorders when conducting an interview or engaging in a conversation with a confidential informant, unless needed as evidence.

Members have no obligation to advise a victim or witness that he or she is being recorded, but may do so at their discretion. When a victim or witness requests they not be recorded, members may consider their request (See Penal Code 632).

Members shall remain sensitive to the dignity of all individuals being recorded and exercise discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy concerns may outweigh any legitimate law enforcement interest in recording. Recording should resume when privacy concerns are no longer at issue unless the member determines that the circumstances no longer fit the criteria for recording.

Informal community interactions differ from "consensual encounters" in which members make an effort to develop reasonable suspicion to detain or probable cause to arrest. To strengthen relationships between police and citizens, members may use discretion regarding the recording of informal, non-enforcement related interactions with members of the community.

## Berkeley Police Department

## Law Enforcement Services Manual

Body Worn Cameras

---

**425.9 ACTIVATION IN CROWD CONTROL SITUATIONS**

During crowd control, protest or mass arrest incidents, members shall use their BWCs consistent with this policy, or when directed by the Incident Commander. The Incident Commander shall document his or her orders to activate in an appropriate report (e.g. Operations Plan or After Action Report).

The limitations outlined in the Intelligence Procedures for First Amendment Activities Policy governing intelligence-gathering procedures for First Amendment activities, apply to the use of BWCs and other recording devices.

Video recording of individuals who are picketing or engaged in peaceful protest will be avoided unless the officer believes a violation of criminal law is occurring, may occur, or if the officer interacts with a participant or third party to the event, or a participant or third party initiates contact with the member.

**425.10 SURREPTITIOUS USE OF THE BWC**

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police, or his/her designee.

Members are prohibited from using department-issued BWCs for non-work related personal activity. BWCs will not be activated in places where members have a reasonable expectation of privacy, such as workplace locker rooms, dressing rooms, members' private vehicles or restrooms.

**425.11 CESSATION OF RECORDING**

Once activated, the member may mute or deactivate their BWC at any time based on their discretion, in the following circumstances:

- (a) Discussion of tactical or confidential information with other law enforcement personnel.
- (b) Where members are on a perimeter or assigned to a static post where the member's direct participation in the incident is complete and they are not actively part of an investigation.
- (c) If it is necessary to discuss issues or concerns with an employee, supervisor, doctor, nurse, or paramedic in private.
- (d) In the member's judgment, a recording would interfere with his or her ability to conduct an investigation.

Decisions regarding the reason for muting or BWC deactivation shall be noted on the recording, or otherwise documented.

# Berkeley Police Department

## Law Enforcement Services Manual

### *Body Worn Cameras*

---

Members shall cease audio/video recording whenever necessary to ensure conversations are not recorded between a person in custody and the person's attorney, religious advisor or physician, unless there is explicit consent from all parties to the conversation. This does not apply to conversations with paramedics or EMTs during their response at a scene, and during transport.

#### **425.12 EXPLOSIVE DEVICE**

Many portable recorders, including BWCs and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

Members believing that the use of a BWC may detonate an explosive device may deactivate their BWC in such cases.

#### **425.13 PROHIBITED USE OF BODY WORN CAMERAS**

Members are prohibited from using a department-issued BWC for personal use and are prohibited from making personal copies of recordings created while on duty or while acting in their official capacity.

Members are prohibited from retaining BWC recordings. Members shall not duplicate or distribute such recordings, except for department business purposes. All such recordings shall be retained at the Department.

Members may not use personally owned recorders (e.g. personal cell phone) to document contacts unless exigent circumstances exist to warrant the use of personally owned recording devices. Regardless, if a member is using a department-issued BWC, and/or another recording device, members shall comply with the provisions of this policy, including retention and release requirements. In every event where members use any recording device aside from or in addition to their department-issued BWC, the member shall document and explain the use and the exigent circumstance in their police report (e.g. the BWC failed and evidence needed to be captured at that moment in time).

Recordings shall not be used by any member for the purpose of embarrassment, intimidation or ridicule.

#### **425.14 PROCESSING AND HANDLING OF RECORDINGS**

To assist with identifying and preserving data and recordings, members shall tag and download recordings in accordance with procedure, and document the existence of the recording in the related case report. Transfers must occur at the end of the member's shift, and any time the member is aware that the storage capacity of the BWC is nearing its limit. In circumstances when the officer cannot complete this task, the officer's supervisor shall immediately take custody of the BWC and be responsible for uploading the data. Officers shall tag each file with the appropriate case/incident number, provide a descriptive title, and select an appropriate category for each recording, using the Axon View app or via the Evidence.com site.

## Berkeley Police Department

## Law Enforcement Services Manual

*Body Worn Cameras*

---

Members are prohibited from intentionally erasing, altering, reusing, modifying or tampering with original audio video recordings. Members may request restriction and subsequent deletion of an accidental recording as described under section 425.16 below.

**425.15 RETENTION REQUIREMENTS**

The Department shall retain all recordings for a minimum of 60 days. Incidents involving consensual contacts, and aid to citizens will be retained for six months, and cold reports will be retained for one year. Recordings of incidents involving use of force by a police officer, detentions, arrests, or recordings relevant to a formal or informal complaint shall be retained for a minimum of two years and one month. Recordings relating to court cases and personnel complaints that are being adjudicated will be manually deleted at the same time other evidence associated with the case is purged in line with the Department's evidence retention policy. Any recordings related to administrative or civil proceedings shall be maintained until such matter is fully adjudicated, at which time it shall be deleted in line with the Department's evidence retention policy, and any applicable orders from the court.

Recordings created by equipment testing or accidental activation may be deleted after 60 days.

**425.16 ACCIDENTAL RECORDING - REQUEST FOR RESTRICTION**

In the event of an accidental or sensitive personal recording of non-departmental business activity, where the resulting recording is of no investigative or evidentiary value, the recording employee may request that the file be restricted pending 60-day deletion by submitting an email request via their chain of command to the Professional Standards Division Captain. The Professional Standards Division Captain will approve or deny the restriction request. In cases where the request is denied, an appeal may be submitted to the Chief of Police, or his/her designee, for restriction authorization. In all cases of restriction requests, a determination should be made within seven calendar days.

**425.17 REVIEW OF RECORDINGS BY A MEMBER**

Members are authorized to review their own BWC video files at any time in furtherance of official business. Such official business includes, but is not limited to, preparing written reports, prior to or while providing testimony in a case or being deposed. Members may review recordings as an evidentiary resource, except as stated in subsection 425.17.1 below. Members shall not retain personal copies of recordings. Members shall not use the fact that a recording was made as a reason to write a less detailed report.

**425.17.1 OFFICER INVOLVED INCIDENTS RESULTING IN GRAVE BODILY INJURY OR DEATH**

- (a) In the event of a critical incident that results in grave bodily injury or death, including an officer-involved shooting or an in-custody death, the BWC of the involved member(s) shall be taken from him or her and secured by a supervisor, commander, or appropriate investigator, as necessary. The involved member(s) shall not access or obtain their footage of the incident until such time as the criminal investigator(s) have reviewed

## Berkeley Police Department

Law Enforcement Services Manual

Body Worn Cameras

---

the video files. It will be the responsibility of the investigation team's supervisor to coordinate with the involved member's supervisor to obtain footage of the incident on behalf of the member.

- (b) Personnel uploading secured BWC video files shall not view the files unless authorized.
- (c) No member involved in a critical incident may view any video recordings prior to an interview by the appropriate criminal investigative unit, and receiving command approval.
- (d) Prior to the conclusion of the criminal interview process, the involved member and/or the member's representative will have an opportunity to review the member's recording(s). The involved member may choose to provide additional information to supplement his or her statement by providing a supplemental statement or separate supplemental document. In no case shall a member alter a report made prior to reviewing the recording.
- (e) The Department acknowledges that recordings taken during critical incidents obtained from BWCs do not necessarily reflect the full extent of the nature of the event or the experience, analysis, training, threat assessment or state of mind of the individual officers(s) in a given incident. Moreover, the recordings, especially video, have limitations and may depict events differently than the events recalled by the involved officer. Specifically, it is understood that the recording device will capture information that may not have been heard and/or observed by the involved officer and that officers may see and hear events that are not captured by the camera.

Officers who are involved in any critical incident where video recordings exist depicting the involved officer, either as a subject officer or witness, shall be provided the following admonishment to the initial interview or submission of the initial written report:

"In this case, there is video evidence that you will have an opportunity to view. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two-dimensional medium and may not capture depth, distance or positional orientation as well as the human eye. Remember, the video evidence is intended to assist your memory and ensure that your statement explains your state of mind at the time of the incident."

#### 425.17.2 SUPERVISORY REVIEW

With the exception of section 425.17.1 above, supervisors are authorized to review relevant recordings any time they are reviewing and approving case reports from their subordinates.

# Berkeley Police Department

Law Enforcement Services Manual

## Body Worn Cameras

---

### 425.17.3 INVESTIGATORY REVIEW

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings support review of the member's performance.

Recorded files may also be reviewed:

- (a) Upon approval by a supervisor, by any member of the Department who is participating in conduct of an official investigation, such as a personnel complaint, an administrative investigation or a criminal investigation.
- (b) Pursuant to lawful process or by court or District Attorney personnel who are otherwise authorized to review evidence in a related case.
- (c) By personnel assigned to investigatory units who are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.
- (d) Upon approval by the Chief of Police, Internal Affairs investigators may review BWC video with a complainant.

Investigators conducting criminal or internal investigations shall:

1. Advise the coordinator to restrict access to the BWC file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols.
3. Notify the coordinator to remove the access restriction when the criminal/internal investigation is closed.

### 425.17.4 TEACHING OR LEARNING TOOL

BWC files may also be reviewed by training staff regarding specific incidents where such files may serve as an internal learning or teaching tool. In the event that videos are intended to be used for training purposes, the involved officer(s) will first be consulted. If he/she objects to the use of the video, such objection shall be submitted to the person in charge of training who shall weigh the value of the video for training against the officer(s) objections and basis for the objection. Should the person in charge of training refuse to grant the request of the involved officer(s), the matter shall be heard by the Chief of Police, or his/her designee, prior to utilizing the video.

### 425.17.5 COB CIVIL CLAIMS AND LAWSUITS

BWC recordings may be reviewed and used by City of Berkeley defense counsel for the purposes of defending the city in civil claims and lawsuits, with the authorization of the Chief of Police, or his/her designee.

## 425.18 RELEASE OF RECORDINGS

All recordings should be reviewed by the Custodian of Records and the City Attorney's Office prior to public release, see General Order R-23 (Release of Public Records and Information).

# Berkeley Police Department

## Law Enforcement Services Manual

### *Body Worn Cameras*

---

In the event that the Police Department or City Department intends to release or publish for any purpose video recordings where officers are captured on video or the video depicts actions taken by them in the course of the performance of their official duties, those officers shall be given written notice of the intention to release or publish said video at least 48 hours prior to such release.

BPD may, without prior notice to involved officers, share video footage with law enforcement, national security, military, or other government agencies outside of Berkeley, when there is reasonable suspicion that criminal activity has occurred or is about to occur.

#### 425.18.1 POLICE REVIEW COMMISSION (PRC)

Access to recorded files will be granted for the purposes of review to the Police Review Commission Officer and/or Investigator investigating a specific complaint where BWC evidence files are available, and are not part of any ongoing criminal investigation.

- (a) The PRC Officer and PRC Investigator will be provided user account access to evidence files through the evidence management system for their use during a complaint investigation and to facilitate viewing by Board of Inquiry members during a Board of Inquiry.
- (b) The PRC Officer and PRC investigator shall not make or create a copy of any evidence file, nor make or allow to be made any audio or video recording of any evidence file while it is being streamed and viewed from the evidence management system.
- (c) The PRC Officer and PRC Investigator shall not allow any unauthorized individuals to view or access evidence files.
- (d) The evidence management system associates an audit trail record with each evidence file, thereby logging the date, time, user, activity, and client IP address occurring during each evidence file access.
- (e) The evidence management system shall only be accessed on City premises.
- (f) The Department retains custody and control of the recordings, and content of the video will be subject to applicable legal standards including, but not limited to the confidentiality requirements of the Public Safety Officers' Procedural Bill of Rights, (Government Code § 3300, et seq., Penal Code § 832.7, and the California Public Records Act; Government Code § 6250, et seq.)

#### 425.18.2 PUBLIC RECORDS ACT (PRA) REQUEST

Access to recorded files will be granted for the purposes of review in response to a public records request, as permitted under Government Code § 6254(f) and BPD General Order R-23 (Release of Public Records and Information). General Order R-23 does not authorize release of investigative files or documents that would constitute an unwarranted invasion of privacy. Circumstances where this might arise in video include footage taken inside a home, a medical facility, the scene of a medical emergency, or where an individual recorded has a "reasonable expectation of privacy."



## Berkeley Police Department

Law Enforcement Services Manual

### *Body Worn Cameras*

---

#### 425.18.3 MEDIA

Access to recorded files will be granted for the purposes of review to media personnel or the general public with permission of the Chief of Police, or his/her designee, subject to General Order R-23 and privacy protections indicated in this policy.

#### **425.19 COMPLIANCE WITH BMC 2.99 ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY**

This policy shall comply at all times with the requirement of BMC 2.99 Acquisition and Use of Surveillance Technology.

#### **425.20 TRAINING REQUIRED**

Officers who are assigned BWCs must complete department-approved training in the proper use and maintenance of the devices before deploying to the field.

As part of a continual improvement process, regular review should be conducted by BPD staff of the training on this policy and the related use of BWCs under this policy. Information resulting from the outcomes of this review shall be incorporated into the City Manager's annual "Surveillance Technology Report" as required under BMC 2.99 Acquisition and Use of Surveillance Technology.

The Department, Police Review Commission and other City Departments shall maintain the confidentiality of Department sworn employee personnel records as required by state and local law. Failure to maintain the confidentiality of Department sworn employee personnel records, whether or not intentional, may subject individuals to civil penalties and discipline, up to and including termination of employment.

**ATTACHMENT 3:**  
**Global Positioning System Tracking Devices**

Surveillance Technology Report GPS Tracker  
To be provided as part of supplemental communications

---

## Surveillance Use Policy - GPS Tracking Devices

### 1301.1 PURPOSE

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals. GPS trackers electronically relay their precise location in real time, and thereby assist BPD in the recovery of evidence and arrest of suspects.

### 1301.2 AUTHORIZED USE

GPS trackers shall only be used during active criminal investigations. GPS trackers shall only be used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

GPS trackers shall only be utilized for law enforcement purposes.

### 1301.3 DATA COLLECTION

Location data may be obtained through the use of a GPS Tracker.

### 1301.4 DATA ACCESS

Access to GPS tracker data shall be limited to Berkeley Police Department (BPD) personnel utilizing the GPS Tracker(s) for active criminal investigations. Information may be shared in accordance with 1301.9 below.

In support of active criminal investigations, BPD personnel may receive GPS tracker data from probation or parole agencies which utilize GPS trackers (e.g. ankle monitors) as a condition of probation or parole.

### 1301.5 DATA PROTECTION

The data from the GPS tracker is encrypted by the vendor. The data is only accessible through a secure website to BPD personnel who have been granted security access.

### 1301.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. Provisions of this policy, including 1301.4 Data Access, 1301.5 Data Protection, 1301.7 Data Retention, 1301.8 Public Access and 1301.9 Third Party Data Sharing serve to protect against any unauthorized use of GPS tracker data. These procedures ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### 1301.7 DATA RETENTION

A GPS Tracker data record consists of date, time, latitude, longitude, map address, and tracker

identification label. This data is stored indefinitely by the vendor. The data does not contain any images, names of subjects, vehicle information, etc.

Tracker data received from the vendor shall be kept in accordance with applicable laws, BPD policies that do not conflict with applicable law or court order, and/or as specified in a search warrant.

**1301.8 PUBLIC ACCESS**

Data collected and used in a police report shall be made available to the public in accordance with department policy and applicable state or federal law.

**1301.9 THIRD-PARTY DATA-SHARING**

Data collected from the GPS trackers may be shared with the following:

- (a) The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- (b) Other law enforcement personnel as part of an active criminal investigation;
- (c) Other third parties, pursuant to a Court Order.

**1301.10 TRAINING**

Training for the operation of the GPS trackers shall be provided by BPD personnel. All BPD personnel shall be provided with this Surveillance Use Policy.

**1301.11 AUDITING AND OVERSIGHT**

Division Captains or their designee shall ensure compliance with this Surveillance Use Policy.

**1301.12 MAINTENANCE**

GPS trackers shall only be obtained with the permission of the Investigations Division Captain or his/her designee. The Investigations Division Captain or his/her designee will ensure the trackers are returned when the mission/investigation is completed.

## GPS TRACKING DEVICES

### A. DESCRIPTION

Global Positioning System (GPS) tracking devices track the movements of vehicles, bicycles, cargo, machinery, other items, and/or individuals.

The Berkeley Police Department currently uses two types of GPS Tracking Devices to track the movements of vehicles, bicycles, or other kinds of property. The manufacturer, 3SI Security Systems, describes them as follows:

1. The "Slap-n-Track" (SNT) tracker tracks vehicles, cargo, and other large assets for long deployments. Offers extended battery life, rugged and weatherproof housing, and optional magnets.
2. The "Electronic Stake Out" (ESO) tracker offers Law Enforcement miniaturized and covertly packaged GPS Tracking Solutions to target property crimes, especially pattern crimes, in their local jurisdictions.

### B. PURPOSE

Global Positioning System (GPS) tracking devices provide precise, real-time location information during the conduct of active criminal investigations. GPS trackers are only used pursuant to a lawfully issued search warrant, or with consent of the owner of the object to which the GPS tracker is attached.

### C. LOCATION

GPS tracking devices shall be deployed in locations consistent with the authority granted by consent or a lawfully issued search warrant or court order.

### D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. GPS Trackers are used in place of expensive, resource-intensive surveillance operations which typically involve multiple officers, often over long periods of time. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with GPS trackers help to ensure no unauthorized use of of GPS tracker data occurs. BPD Policy 1301 Surveillance Use Policy – GPS Tracking Devices ensure the use of GPS trackers and the resulting data are not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1301 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - GPS TRACKING DEVICES

---

**E. MITIGATION**

Data from a GPS tracker is encrypted from the vendor. Data shall be maintained in a secure, non-public location, such as locations requiring security access or badge access, thereby safeguarding the public from any impacts identified in subsection (D).

**F. DATA TYPES AND SOURCES**

A GPS tracker data record consists of date, time, latitude, longitude, map address (derived by using latitude, longitude and Google maps), and tracker identification label. The data does not contain any images, names of subjects, vehicle information, etc.

**G. DATA SECURITY**

Data from a GPS tracker is encrypted by the vendor on secure servers. The data is only accessible through a secure website to BPD personnel who have been granted security access. Captains whose Divisions utilize GPS trackers are responsible for ensuring compliance with the procedures for utilizing GPS Trackers.

**H. FISCAL COST**

The initial cost of the GPS trackers totaled \$4,335.

- Between 2015-present BPD purchased 5 GPS "ESO" trackers for \$2,250 (\$450 each).
- In 2017 BPD purchased 3 GPS "SNT" trackers for \$2,085 (\$695 each).

The annual cost for the GPS data service totals \$1,920.

- The annual data service for the five ESO trackers is \$1,020 (\$204 each).
- The annual data service for the three SNT trackers is \$900 (\$300 each).

Personnel costs are minimal in that the GPS trackers are used as a resource during normal working hours.

GPS trackers are funded through the Investigations Division's general budget.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

Data collected from the GPS trackers may be shared with the following:

- a. The District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- b. Other law enforcement offices as part of a criminal investigation;
- c. Other third parties, pursuant to a Court Order.

**1301 APPENDIX A**

**BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - GPS TRACKING DEVICES**

---

**J. ALTERNATIVES**

An alternative to the use of GPS trackers is to conduct resource-intensive surveillance operations utilizing numerous personnel over extended periods of time.

**K. EXPERIENCE OF OTHER ENTITIES**

The use of GPS tracker technology is common amongst law enforcement agencies throughout the country.



ATTACHMENT 4:  
Automated License Plate Readers

Surveillance Technology Report Automated License Plate Reader  
To be provided as part of supplemental communications

---

## Surveillance Use Policy - ALPR

### 1302.1 PURPOSE

This Surveillance Use Policy is issued in compliance with BMC 2.99, and incorporates by reference language from the Berkeley Police Department ALPR Policy #422 and adds elements as required by BMC 2.99.

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review. (Ref. policy 422.2)

### 1302.2 AUTHORIZED AND PROHIBITED USES USE

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53). (Ref. policy 422.4)

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used to support a patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

### 1302.3 DATA COLLECTION

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law. (Ref. policy 422.5)

### 1302.4 DATA ACCESS

- (a) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (b) No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so.
- (c) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

---

### **1302.5 DATA PROTECTION**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref. policy 422.6):

- (a) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (b) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
- (c) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (d) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

### **1302.6 CIVIL LIBERTIES AND RIGHTS PROTECTION:**

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures described within this policy (Data Access, Data Protection, Data Retention, Public Access and Third Party Data Sharing) protect against the unauthorized use of ALPR data. These policies ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

### **1302.7 DATA RETENTION**

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data. Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT) department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence. (Ref. policy 422.5)

- 
- (a) Collected images and metadata of hits will not be stored for more than 365 days. Metadata of reads will not be stored for more than 30 days. Images of reads will not be transferred to the server.

### **1302.8 PUBLIC ACCESS**

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. (Ref. policy 422.6 (a))
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question. (Ref. policy 422.6 (b))

### **1302.9 THIRD-PARTY DATA-SHARING**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. ALPR data is subject to the provisions of BPD Policy 415, and hence may not be shared with federal immigration enforcement officials.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager. (Ref. policy 422.6 (e))

### **1302.10 TRAINING**

Training for the operation of ALPR Technology shall be provided by BPD personnel. All BPD employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

### **1302.11 AUDITING AND OVERSIGHT**

ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually. (Ref. policy 422.6 (g))

### **1302.12 MAINTENANCE**

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data. (Ref. policy 422.3)

#### **1302.12.1 ALPR ADMINISTRATOR**

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53) (Ref.

policy 422.3.1):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

## AUTOMATED LICENSE PLATE READER (ALPR) DEVICES

### A. DESCRIPTION

Automated License Plate Readers (ALPRs) are high-speed, computer controlled camera systems that are typically mounted on Berkeley Police Department Parking Enforcement Vehicles.

ALPRs capture license plate numbers which come into view, along with the location, date and time. The data, which includes a photo of the front or the back of the car displaying the license plate, is then uploaded to a central server.

### B. PURPOSE

The Berkeley Police Department's Parking Enforcement Unit utilizes vehicles equipped with ALPRs to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's also access information in the California Law Enforcement Telecommunications System's (CLETS) Stolen Vehicle System (SVS) database, which provides information on matches for stolen and wanted vehicles.

The Berkeley Police Department's Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates, and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding parking citation fees.

### C. LOCATION

Parking Enforcement vehicles travel throughout the city; using the ALPRs as described above.

### D. IMPACT

The Berkeley Police Department is dedicated to the most efficient utilization of its resources and services in its public safety endeavors. The Berkeley Police Department recognizes the need to protect its ownership and control over shared information and to protect the privacy and civil liberties of the public, in accordance with federal and state law. The procedures utilized with ALPR Units will help to ensure unauthorized use of its data. The procedures will ensure the data is not used in a way that would violate or infringe upon anyone's civil rights and/or liberties, including but not limited to potentially disparate or adverse impacts on any communities or groups.

1302 APPENDIX A

**BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES**

---

**E. MITIGATION**

All saved data will be safeguarded and protected by both procedural and technological means which are implemented to safeguard the public from any impacts identified in subsection (D). See subsection (G) for further.

**F. DATA TYPES AND SOURCES**

Photographs of license plates and location data may be obtained through the use of ALPR Units.

**G. DATA SECURITY**

The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
2. Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action and parking enforcement.
3. Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
4. Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.

**H. FISCAL COST**

In 2015, Public Works brought an ALPR Contract to City Council. Council approved a contract for Public Works to buy five Genetec ALPR Units with PCS Mobile communication, for a pilot program for \$450,000.

In 2017, after success with the program, City Council approved an amendment to the contract, allowing Public Works to purchase 15 more ALPR Units for Parking Enforcement vehicles, and to continue its use of PCS Mobile, for 1,200,000. The money was allocated from the goBerkeley/Federal Highway Administration Parking Meter Fund.

Yearly service for the ALPR Units includes warranties, hosting services, cellular connection, mobile computing, and training which varies. The costs through fiscal year 2022 are currently estimated at \$1,175,000.



## 1302 APPENDIX A

BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES

---

Personnel costs are minimal in that the ALPR Units are used as a resource during normal working hours.

**I. THIRD PARTY DEPENDENCE AND ACCESS**

1. Vendor Access-Scofflaw Enforcement: The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:
  - a. All data captured by the ALPR is stored on the booting vehicle's laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.
  - b. When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.
2. Vendor Access-General Parking Enforcement and goBerkeley Program: The contracted vendor for the City's Parking Enforcement ALPR is currently Genetec. The city uses Genetec ALPRs to support efficient enforcement of posted time limit parking and Residential Preferential Parking permits.
  - a. In addition, Genetec periodically provides reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that the City's program can analyze data about parking demand. These reports do not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports consist of completely anonymized information, using identification numbers that are not associated with a particular license plate or registered owner.
  - b. The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and Residential Permit Pass (RPP) area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.
3. Department of Information Technology Access: Technical support and assistance for ALPR's is provided by the City of Berkeley's Department of Information Technology (IT) and associated ALPR system providers/vendors as identified herein. IT staff who

**1302 APPENDIX A****BERKELEY POLICE DEPARTMENT SURVEILLANCE ACQUISITION REPORT - AUTOMATED LICENSE PLATE READER DEVICES**

---

do not have the proper clearance and training do not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT provides initial infrastructure set-up, and continued systems support as needed to ensure efficient and accurate performance of the ALPR hardware and software. Only IT staff members who have successfully undergone DOJ background checks and training are authorized by the Chief of Police to view specific ALPR records.

4. Other Law Enforcement Agency Access: ALPR data may only be shared with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55). Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
5. Member Access: No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training. No ALPR operator may access CLETS data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.
6. Public Access: Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law. Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.

**J. ALTERNATIVES**

None.

**K. EXPERIENCE OF OTHER ENTITIES**

The use of ALPR technology is common amongst law enforcement agencies throughout the country, in support of parking enforcement, and law enforcement criminal investigations.

## Automated License Plate Readers (ALPRs)

### 422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

### 422.3 ADMINISTRATION

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

#### 422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### 422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use,

---

or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.
- (b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert

#### **422.5 .DATA COLLECTION AND RETENTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review.

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT Department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

- (a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.
- (b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not

showing violations will not be transferred to the server.

#### **422.6 ACCOUNTABILITY**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

For security or data breaches, see the Records Release and Maintenance Policy.

#### **422.7 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  - 1. The name of the agency.
  - 2. The name of the person requesting.
  - 3. The intended purpose of obtaining the information.

- 
4. The related case number.
  - (b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.
  - (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

#### **422.8 SCOFFLAW ENFORCEMENT**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

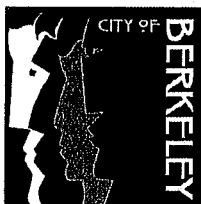
The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking

enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

**ATTACHMENT 5:**  
**Police Review Commission Communication**





Police Review Commission (PRC)

September 11, 2019

To: Honorable Mayor and Members of the City Council  
From: George Perezvelez, Chairperson, Police Review Commission  
Re: Proposed Berkeley Police Department Policy 422, Automated License Plate Readers

Summary: This memo is to inform you of the Police Review Commission's qualified approval of the BPD's proposed policy for the use of Automated License Plate Readers (ALPRs).

Background: The BPD submitted the ALPR policy, Policy 422, to the PRC for review, along with the Surveillance Use Policy and the Surveillance Acquisition Report (Policy 1302 and Appendix A) for these devices. This process was undertaken in advance of BPD submitting these items to the City Council as required by the Surveillance Technology Use and Community Safety Ordinance (B.M.C. Ch. 2.99).

These policies were first considered by the full Commission, which then referred them to its Lexipol Policies Subcommittee. In response to feedback from the PRC and the Subcommittee, the BPD revised the proposed policy, which was reviewed by both bodies. At various stages, the PRC and the subcommittee had the opportunity to hear from and ask questions of Police Chief Greenwood and other members of the BPD, and Deputy City Attorney Chris Jensen. The PRC also heard input from representatives of Media Alliance and Oakland Privacy.

Final action: At its September 4, 2019 meeting, the PRC voted to approve for submission to the City Council for your review and discussion the version of Policy 422 that is attached here, with two caveats. First, there was concern among some commissioners that the ALPR was originally acquired for the purpose of parking enforcement and that this policy represents an expansion of that function. If this is not what the Council had in mind, then this policy should be modified accordingly. Second, Section 422.4(c) of the policy does not adequately define what constitutes a "crime scene."

Finally, the Commission wishes to remind the Council that they will see actual use of the ALPR technology under the reporting mechanism in place in the Surveillance Technology Use and Community Safety Ordinance.

Honorable Mayor and Members of the City Council  
Proposed Berkeley Police Department Policy 422, Automated License Plate Readers  
September 11, 2019  
p. 2

The above action was approved by the following vote: Moved/Seconded  
(Perezvelez/Mikiten) -- Ayes: Calavita, Chang, Leftwich, Mikiten, Perezvelez,  
Ramsey; Noes: Earnest, Mizell; Abstain: Allamby; Absent: None.

Attachment: Revised Policy 422

cc: Dee Williams-Ridley, City Manager  
Andrew Greenwood, Chief of Police  
David White, Deputy City Manager  
PRC Commissioners

## Automated License Plate Readers (ALPRs)

### 422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

### 422.2 POLICY

The policy of the Berkeley Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

### 422.3 ADMINISTRATION

Any installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Investigations Division Captain. The Investigations Division Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

#### 422.3.1 ALPR ADMINISTRATOR

The Investigations Division Captain, or his/her designee, shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- (b) Training requirements for authorized users.
- (c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- (d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- (e) The title and name of the current designee in overseeing the ALPR operation.
- (f) Ensuring this policy and related procedures are conspicuously posted on the City's website.

### 422.4 USE OF THE ALPR

An ALPR shall only be used for official law enforcement business.

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use,

---

or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

- (a) An ALPR may be used by Berkeley Police Department Parking Enforcement for parking and scofflaw enforcement.
- (b) An ALPR may be used to support criminal investigations. Reasonable suspicion or probable cause is not required before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

No ALPR operator may access California Law Enforcement Telecommunications System (CLETS) data unless otherwise authorized to do so. If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

#### **422.5 DATA COLLECTION AND RETENTION**

All data and images gathered by an ALPR are for the official use of the Berkeley Police Department. Such data may contain confidential CLETS information and is not open to public review. ~~ALPR information gathered and retained by this department may be used and shared with prosecutors or other law enforcement agencies only as permitted by law.~~

The Investigations Division Captain, or his/her designee, is responsible for ensuring proper collection and retention of ALPR data.

Technical support and assistance shall be provided by the City of Berkeley's Information Technology (IT Department and associated ALPR system providers/vendors as identified below. IT staff will not have the ability to access or view individual records or reports, as they may contain CLETS information they are not authorized to receive. IT's role will be limited to providing initial infrastructure set-up, unless particular IT staff members have been cleared by DOJ background checks and authorized by the Chief of Police to receive ALPR records.

All ALPR data downloaded to the server should be stored for a minimum of one year (Government Code § 34090.6) and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

- (a) Collected images and metadata of reads showing violations will not be stored for more than 365 days.

- 
- (b) Metadata of reads showing violations will be stored for up to 30 days. Images of reads not showing violations will not be transferred to the server.

#### **422.6 ACCOUNTABILITY**

All saved data will be safeguarded and protected by both procedural and technological means. The Berkeley Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- (a) Non-law enforcement requests for access to stored ALPR data shall be processed according to the Records Maintenance and Release Policy in accordance with applicable law.
- (b) Non-law enforcement requests for information regarding a specific vehicle's license plate may be honored when the requester is the registered owner of the vehicle in question, and when providing such information will not invade the privacy of a third party. The requestor in such cases must provide acceptable proof of his or her identity and of ownership of the vehicle in question.
- (c) All ALPR data downloaded to any workstation or server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).
- (d) Berkeley Police Department members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action or parking enforcement.
- (e) Aggregated ALPR data not related to specific criminal investigations shall not be released to any local, state or federal agency or entity without the express written consent of the City Manager.
- (f) Measures will be taken to ensure the accuracy of ALPR information. Errors discovered in ALPR data collected by ALPR units shall be marked, corrected or deleted in accordance with the type and severity of the error in question.
- (g) ALPR system audits will be conducted by the Professional Standards Bureau's Audit and Inspections Sergeant on a regular basis, at least biannually.

For security or data breaches, see the Records Release and Maintenance Policy.

#### **422.7 RELEASING ALPR DATA**

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

- (a) The agency makes a written request for the ALPR data that includes:
  1. The name of the agency.

2. The name of the person requesting.
  3. The intended purpose of obtaining the information.
  4. The related case number.
- (b) The request is reviewed by the Investigations Division Captain, or his/her designee, and approved before the request is fulfilled.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

ALPR data is subject to the provisions of the Berkeley Police Department's Immigration Law Policy, and hence may not be shared with federal immigration enforcement officials.

#### **422.8 SCOFFLAW ENFORCEMENT**

The Berkeley Police Department uses ALPR technology in the Parking Enforcement Unit for parking and scofflaw enforcement.

The Parking Enforcement Unit will utilize vehicles equipped with ALPR units to conduct enforcement of posted time limits in commercial areas and Residential Preferential Parking (RPP) permit areas. These ALPR's will also access information in the DMV's Stolen Vehicle System (SVS) database for wanted and stolen vehicles.

The Scofflaw Enforcement program (often referred to as the "booting" program) utilizes an ALPR to scan license plates and check the scanned "reads" against a list of vehicles which have five or more outstanding parking citations exceeding 30 days old. Typically, upon a confirmed "hit," the vehicle is immobilized with a "boot", or towed, and the owner has to pay the outstanding citations and fees in order to release the boot and/or recover their car from storage. This allows the City to recover outstanding citation fees.

The contracted vendor for the City's Scofflaw Enforcement program is currently Paylock. Paylock stores data on a secure server, and provides access to authorized personnel via Paylock's "Bootview" secure website, as described below:

- (a) All data captured by the ALPR is stored on the laptop for 30 days, and is only accessible during that period via the ALPR proprietary software. This includes reads, hits, and photographs associated with each.

When a car is booted and/or towed, the read, hit and photographic data relating to the booting and/or towing of scofflaw vehicles is uploaded to Paylock's secure server. No other data is uploaded to Paylock's secure server.

The City's Parking Enforcement ALPR vendor (currently Genetec) will periodically provide reports to the City of Berkeley Transportation Division's "goBerkeley" parking management program so that it can analyze data about parking demand. These reports will not contain any information about a vehicle's license plate number, the name of the registered owner, address of registered owner, or any other information gleaned from the license plate number associated

with a particular vehicle. Rather, the reports will consist of 100 percent anonymized information using identification numbers that are not associated with a particular license plate or registered owner.

The reports will provide only the date, time, location, approximate address, "goBerkeley" blockface ID, and RPP area in which a vehicle was observed. If a citation was not issued for an RPP or other time limit violation, the report may also provide the reason a parking enforcement officer concluded there was no parking violation, e.g., RPP visitor pass, disabled placard or license plate, etc.

