

1 PETER BIBRING (State Bar No. 223981)  
pbibring@aclu-sc.org  
2 ACLU FOUNDATION OF SOUTHERN  
3 CALIFORNIA  
1313 West Eighth Street  
4 Los Angeles, California 90017  
Telephone: (213) 977-9500  
5 Facsimile: (213) 977-5299

6 JENNIFER LYNCH (State Bar No. 240701)  
jlynch@eff.org  
7 ELECTRONIC FRONTIER FOUNDATION  
8 815 Eddy Street  
San Francisco, CA 94109  
9 Telephone: (415) 436-9333  
10 Facsimile: (415) 436-9993

11 Attorneys for Petitioners

12  
13 **SUPERIOR COURT OF CALIFORNIA**

14 **IN AND FOR THE COUNTY OF LOS ANGELES**

15  
16 AMERICAN CIVIL LIBERTIES UNION )  
FOUNDATION OF SOUTHERN )  
17 CALIFORNIA and ELECTRONIC FRONTIER )  
FOUNDATION, )

18 )  
19 )  
20 )  
21 )  
22 )  
23 )  
24 )  
25 )  
26 )  
27 )  
28 )

Petitioners,

v.

COUNTY OF LOS ANGELES, and the )  
LOS ANGELES COUNTY SHERIFF'S )  
22 DEPARTMENT, and the CITY OF LOS )  
23 ANGELES, and the LOS ANGELES POLICE )  
DEPARTMENT, )

Respondents.

Case No.: BS143004

**DECLARATION OF PETER BIBRING  
IN SUPPORT OF MEMORANDUM OF  
POINTS AND AUTHORITIES IN  
SUPPORT OF PETITION FOR WRIT  
OF MANDAMUS**

**EXHIBITS A-D**

[Gov. Code §§ 6250, *et seq.*;  
Civ. Proc. Code §§ 1085, *et seq.*]

Hearing Date: March 21, 2014

Hearing Time: 9:30 a.m.

Place: Department 86

Honorable Joanne O'Donnell

1 **DECLARATION OF PETER BIBRING**

2 I, Peter Bibring, hereby declare:

3 1. I am an attorney of record licensed to practice before the courts of the State of  
4 California. This declaration is submitted in support of the amicus brief filed by the American Civil  
5 Liberties Union of Southern California (“ACLU/SC”) and Electronic Frontier Foundation (“EFF”) in  
6 the above-captioned matter. I have personal knowledge of the facts set forth below and if called  
7 to testify, I could and would do so competently.

8 2. Attached as Exhibit A hereto are documents received by the ACLU/SC from the  
9 Los Angeles Sheriff’s Department (“LASD”) in response to the ACLU/SC’s September 18, 2012  
10 request for records, as described in paragraph 33 of the Petition.

11 3. Attached as Exhibit B hereto are documents received by EFF from LASD in  
12 response to EFF’s August 30, 2012 request for records, as described in paragraphs 12, 13 and 15 of  
13 the Petition.

14 4. Attached as Exhibit C hereto are selected documents received by the ACLU/SC  
15 from the Los Angeles Police Department in response to the ACLU/SC’s request for records, as  
16 described in paragraph 41 of the Petition. Out of the 31 documents received by the ACLU, 22  
17 involve the logistics of acquiring ALPRs (requests for proposals, purchase orders, invoices,  
18 shipping manifests, quarterly expenditure statements) or manufacturer’s user manuals — this  
19 selection includes all documents other than those two categories. This selection includes the  
20 following documents:

- 21 a. Email from Stephen Dolan re ALPR vehicle operating instructions (1 page)
- 22 b. Web page for PIPS Technology ALPR system (1 page)
- 23 c. Email from “TacTech” re ALPR vehicle operating instructions (apparently  
24 identical to #1, above)
- 25 d. LAPD Major Crimes Division Standards and Procedures (related to  
intelligence investigations generally, does not mention ALPRs) (37 Pages)
- 26 e. LAPD Manual Vol. 5, Records Retention Policies. (2 pages)
- 27 f. Los Angeles Municipal Code, Records Retention Sections (16 pages)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- g. Memorandum of Understanding between City of Los Angeles and University of Southern California (21 pages)
- h. Special Enforcement Vehicle Check-out Logs (4 pages)
- i. Spreadsheet of Deployment of ALPRs (2 pages)

5. Attached as Exhibit D is a document retrieved from the City of Los Angeles website authored by members of the Los Angeles Police Department entitled Transmittal of the Extension for the 2009 Los Angeles Smart Policing Project, *available at* [http://www.lapdpolicecom.lacity.org/031213/BPC\\_13-0088.pdf](http://www.lapdpolicecom.lacity.org/031213/BPC_13-0088.pdf) (last visited January 24, 2014).

I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this 24th day of January, 2014 in Los Angeles, California.

  
PETER BIBRING

# **Exhibit A**



*Berry D. Baca, Sheriff*

*County of Los Angeles*  
**Sheriff's Department Headquarters**

*4700 Ramona Boulevard  
Monterey Park, California 91754-2169*



October 15, 2012

Yaman Salahi  
American Civil Liberties Union  
1313 West Eighth Street  
Los Angeles, California 90017

Re: Follow-up to Public Act Request Regarding Surveillance Technologies

Dear Mr. Salahi:

This letter is in response to your letter dated September 18, 2012, regarding the denial of the specific records under the Public Records Act (PRA) request you submitted on August 10, 2011. Listed below are the documents of concern:

- All policies, procedures, and practices governing use by the department of GPS Tracking Devices and/or ALPRs.
- All policies, procedures, training, and practices governing and/or limiting the purposes for which information obtained through use of GPS Tracking Devices and/or ALPRs may be used by the department or shared with other (federal, state or local) government agencies or non-governmental entities.
- All data policies relating to the maintenance and retention of information obtained through GPS Tracking Devices and/or ALPRs, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, and circumstances under which they are deleted.

**Response:** Enclosed are the responsive documents to your request: Los Angeles County Sheriff's Department, Field Operations Directive 09-04 – Automated License Plate Recognition (ALPR) System; Department Policies and Guidelines; Los Angeles County Sheriff's Department, Century Station Order #72 – Advanced Surveillance and Protection (ASAP).

*A Tradition of Service Since 1850*

If you have any questions, please contact Pam Vanover of the Discovery Unit at (323) 890-5439.

Sincerely,

LEROY D. BACA, SHERIFF

A handwritten signature in black ink, appearing to read "Judy A. Gerhardt". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Judy A. Gerhardt, Lieutenant  
Risk Management Bureau

## **CENTURY STATION ORDER #72**

### **TITLE: ADVANCED SURVEILLANCE AND PROTECTION (ASAP)**

---

**JAMES J. HELLMOLD, CAPTAIN**  
May 10, 2008

---

#### **PURPOSE:**

The purpose of this Station Order is to outline the Policies, Procedures, and protocols for using video surveillance and advanced technologies in the field, known as Advanced Surveillance and Protection (ASAP).

#### **POLICY:**

The use of video surveillance and other advanced technologies in the field shall be guided by the United States Constitution and all applicable laws relating to a person's reasonable expectation of privacy. Specific guidelines for the practical use of ASAP technologies are guided by Department Policy, common sense, and fairness.

The Century Station Advanced Surveillance and Protection (ASAP) plan consists of the following technologies: video surveillance (recorded via automated computer server), acoustic gunshot detection with digital mapping, gunshot detection cameras, ASAP radio cars equipped with automatic license plate recognition (ALPR), fixed ALPR cameras, and other advanced technologies benefitting public and officer safety.

The primary purpose of the Century Station ASAP plan is to strengthen public safety and address quality of life issues in the community. This will be accomplished by streaming advanced technologies into the Century Station Dispatch Command Center to provide deputies with real-time intelligence in the field, and video evidence for successful prosecution when deputies are made aware of a crime. Use of video surveillance and other ASAP technologies by Department personnel shall be restricted solely for primary law enforcement functions.

Recorded information used for evidentiary purposes or requested by court order shall be booked into evidence in accordance with MPP §5-04/000. All data, including routine recordings, activity logs, and procedures regarding the CCTV system shall not be considered public information under the Public Records Act.

## **LOGGING PROCEDURES:**

Sworn personnel may request a copy of a video recording when it relates directly to possible criminal activity. The procedures shall be as follows:

*When a deputy sheriff becomes aware of video involving possible criminal activity recorded by the Century ASAP system, he/she shall notify the Watch Deputy.*

*The video shall be saved by the Watch Deputy or (ASAP trained personnel) under Century Station Shared Files (1-cen/sharedfiles/asap/videoevidence). Subsequently, a copy of the same video shall be burned onto a DVD for evidentiary purposes.*

*The video shall be saved and logged/named under the corresponding year, month, day, time of incident, and brief description of the incident. For example, the first saved video of a Lynwood shooting incident on January 5, 2008 at 1932 hours would be saved and identified in the following manner and sequence: 2008-01-05-1932-Lynwood 245*

*A copy of the recording shall be burned onto DVD by the Watch Deputy, clearly marked with the appropriate file number, and booked into evidence under normal protocols. The booked DVD will be considered and identified as the "original item of evidence."*

If there are no ASAP trained personnel on-duty to save a copy of the video, the requesting deputy shall simply email the Century Station ASAP liaison or Detective Bureau Commander with the file name, location, date, and time of the video. The ASAP liaison will provide a copy of the recording on the next business day.

ASAP surveillance cameras are set-up to record 24 hours per day, storing the recorded video footage on a station server. The current recording capacity for Century Station ASAP server is approximately four days after which time the recorded footage is recorded over. Therefore, the watch commander shall be notified if an immediate copy of the recording is required and there are no ASAP trained personnel available to save the video.

## **AUTOMATIC LICENSE PLATE RECOGNITION (ALPR):**

The wanted vehicle database (stolen, felony, etc.) for the ALPR system is updated 3 times per day, and may contain outdated information. Therefore whenever an ALPR camera identifies a wanted vehicle, desk personnel shall confirm the wants via MDT, CAD, or SCC prior to initiating law enforcement action. Once the vehicle's wanted status is confirmed, deputies will coordinate responding field units pursuant to established Department policy and procedures.



September 5, 2012

## **AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM**

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles, as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists". The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database six times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) or Mobile Digital Computer (MDC), prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server within seconds of the scans occurring. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Most mobile ALPR units do not have a "continuous" connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at the beginning and end of their shift to ensure they have the latest informational data available. If the ALPR system is integrated with an MDC, it is possible for the user to update their data via the unit's cellular connection in the field.

### **BOSS (Back Office System Server)**

The BOSS server is where all the stored ALPR data resides. Within the server are the "hotlists," which are deployed and used to compare the license plates that are scanned by the ALPR cameras. The "hotlists" are maintained by the ASAP (Advanced Surveillance and Protection) Unit and are set-up to refresh automatically. There are a few cases which specific hotlists have been set-up for certain units and they have to be updated manually (most of these lists are covert hotlists and the user is not notified of the "hit"). The primary use of the server is for storage of the license plate data captured. Currently, we maintain approx. (2) years' worth of license plate data from all of our LASD ALPR cameras. Detectives and other investigative resources can utilize the BOSS database in searches for full or partial license plate information. Additionally, we have set-up links to query other LA County police agencies approx. 26 at this time, and are in the process of setting up and expanded ability to search other county law enforcement agencies with ALPR such as San Bernardino County Sheriff and Riverside County Sheriff.

## **Department Policies and Guidelines**

There are no written guidelines as to how to use the data. The policy of how we use Department resources (data) is listed below. Keep in mind data is often used as a "lead" to glean further information on an active investigation that law enforcement handles.

Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

### **3-07/200.00 SHERIFF'S DATA NETWORK (SDN)**

The Sheriff's Data Network (SDN) central hub is at the Sheriff's Headquarters Building and is under the administration of Data Systems Bureau.

The Sheriff's Data Network is a high speed network connecting all Sheriff's Department facilities and participating Los Angeles County municipal police departments. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, LA Net, CLETS, and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJIS, LARCIS, CWS, CCHRS, RAPS, FMS, Cal Gangs (Formerly GREAT), CWTAPPS, JDIC and the Department's Intranet Server. For an up-to-date list of applications available on the Sheriff's Data Network, contact the Data Systems Bureau Help Desk.

### **3-07/210.00 PERMISSIBLE USE**

The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

### 3-07/220.00 PROHIBITIONS

Employees shall not add, alter, copy, damage, delete, move, modify, tamper with or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- Devise or execute any scheme or artifice to defraud, deceive, destroy or extort,
- Wrongfully control or obtain money, property, or data,
- Disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network,
- Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

Unless specifically authorized by Data Systems Bureau, Department employees shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software.

#### Employees shall not do any of the following without the required authorization:

- Access or allow access to another to obtain, alter, or prevent access to stored electronic communications,
- Use electronic communications to capture or open electronic communications of another, or access files without permission of the owner,
- Damage hardware, software, or other communications equipment or interfere with functionality,
- Attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission,
- Modify or delete any file, folder or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records,
- Access the files belonging to another for non-business purposes,
- Use someone else's USERID, password or access another person's files, or retrieve stored communications without authorization,
- Modify the hardware or software configuration on any computer,
- Use electronic communications to transmit (upload) or receive (download):
  - Any communication violating any applicable laws, regulations, or policies,
  - Proprietary or confidential Department information,
  - Chain letters,
  - Material that would be offensive to a reasonable person.
- Transmit any electronic message in violation of file size restrictions,
- Use Department computer equipment or network to send or receive electronic communications for non-Department business,
- Use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the County or third parties,

- Send or receive commercial software in violation of its license agreement,
- Copy personal files, programs, or images into any Department computer without authorization from their unit commander,
- Send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual or contain derogatory racial or religious content,
- Establish any hidden or misidentified links on any web page,
- Send or forward messages which have been altered in order to deceive the receiver as to the original content,
- Use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use,
- Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment,
- Use electronic communications in competition with commercial services to individuals or organizations outside the Department,
- Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering,
- Give out employee personal information such as home address and/or telephone numbers.

### 3-07/220.20 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT

- As an employee of the Los Angeles County Sheriff's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 - 11144 and 13301 - 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:
- "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."
- California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any employee who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

**3-07/250.00 LASD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES**

Employees will be responsible for reading and signing the Sheriff's Department "User Acknowledgment of Electronic Communications Policy" form before obtaining authorization to access the Sheriff's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of sergeant or higher. An employee may request authorization to access the Sheriff's Data Network by submitting the request as described under the manual section entitled, Data Communications Management (section 3-07/230.00), and attaching the signed user acknowledgment form.

**User Acknowledgment of Electronic Communications Policy**

I understand that the Los Angeles County Sheriff's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures, section 3-07/200.10 through section 3-07/250.00 inclusive. I have received a copy of these sections of the Manual of Policy and Procedures.

I understand that I must not have an expectation of privacy when using County electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized employees.

By signing this form, I agree to abide by all policies, including state statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions, and that disciplinary actions may result from not abiding by these policies. I also agree to give authorized persons, including supervisors, auditors, and investigators access to my equipment, software, and files at reasonable times for the purposes of investigating compliance.

User Name (PRINT)  
Date

User Signature

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, section 3-07/200.10 through section 3-07/250.00 inclusive, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands' this policy.

Supervisor's Name (PRINT)  
Date

Supervisor's Signature

\* Attached is our Field Operations Directive as to how we utilize ALPR in the field \*

We do not have user manuals for members of the Department. We train personnel in groups utilizing the train the trainer methodology. Both interfaces of the ALPR system are intuitive and do not require extensive training.

Retention is currently limited by the size of the data stored. As we expand the number of ALPR units, we additionally have to minimize the retention of the data we keep. Currently, we would prefer to retain data indefinitely but this will change if we cannot keep up with the increasing data storage requirements. There is no national or state mandate specifically for ALPR data retention (in California) and we have looked at similar standards, such as video, which is currently (2) years.

Sergeant John Gaw  
LASD / Technical Services Division  
Communications and Fleet Management Bureau (CFMB)  
Advanced Surveillance and Protection Unit (ASAP)  
12440 East Imperial Highway, #130  
Norwalk, CA 90650  
(562) 345-4476 / Office  
[jlqaw@lasd.org](mailto:jlqaw@lasd.org)  
[asap@lasd.org](mailto:asap@lasd.org)  
<http://intranet.lasd.sheriff.sdn/intranet/announcements/ASAP/ASAP.shtml>  
[www.comptonasap.com](http://www.comptonasap.com)  
<http://www.lasd.org/sites/ASAP/index.html>  
<http://www.youtube.com/user/LACountySheriff>



---

# Los Angeles County Sheriff's Department

## FIELD OPERATIONS DIRECTIVE



Field Operations Support Services, (323) 526-5760

---

FIELD OPERATIONS DIRECTIVE: 09-04

DATE: August 17, 2009

ISSUED FOR: OFFICE OF HOMELAND SECURITY  
FIELD OPERATIONS REGIONS  
DETECTIVE DIVISION  
TECHNICAL SERVICES DIVISION

### AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM

#### Purpose

The purpose of this directive is to establish procedural guidelines and responsibilities of personnel and units utilizing the Automated License Plate Recognition (ALPR) system. As with any technical system, adherence to standards and procedures is a key element to the success of the system.

#### Background

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans

Originally Issued: 08-17-09  
Revised:  
Latest Revision:



captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists." The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database three times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

### Policy and Procedures

Units utilizing ALPR technology shall publish unit level policy to govern procedures on ALPR usage as well as the syncing of data between the mobile ALPR units and the ALPR server.

Mobile ALPR unit users receiving an alert that a vehicle is stolen, wanted or has a warrant associated with it shall immediately confirm the status of the vehicle by running the license plate either manually via the MDT/CAD or over the radio via SCC, unless compelling circumstances are present or officer safety issues make it unsafe to do so. In such cases, deputies shall confirm the status of the wanted vehicle as soon as possible. When requesting SCC to confirm the status of an ALPR alert, the deputy shall

advise SCC the request is for an ALPR alert on a vehicle.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a "Code-9" due to an ALPR alert on a stolen vehicle, deputies shall advise SCC they are following a vehicle due to an ALPR stolen vehicle alert (i.e. "142F1 is code 9 on 10-29V ALPR hit") prior to receiving a secondary confirmation by MDT/SCC.

Deputies shall adhere to the Department's pursuit policy as described in the Manual of Policy and Procedures § 5-09/210.00. SCC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via SCC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

Any incident associated with the ALPR system shall be documented using a secondary ALPR statistical code. The statistical code shall go on the classification line of the Incident Report (SH-R-49) and in the MDT clearance. Additionally, any vehicle recovered using the ALPR system shall have "ALPR RECOVERY" written across the top of the CHP-180 and the secondary ALPR statistical clearance code will be entered into the MDT clearance log. ALPR statistical codes cannot be used for the issuance of an URN number, but shall be used as a secondary statistical clearance code.

Please ensure the following stat codes are used:

835 - ASAP - ALPR/MOBILE  
836 - ASAP - ALPR/FIXED CAMERA

Examples:

Personnel making an arrest due to an ALPR alert shall enter "835" or "836" as a secondary statistical clearance code in their MDT Log Clearance and on the Classification line of the SH-R-49 report form.

Personnel recovering a stolen vehicle with no suspect in custody shall write "ALPR-CAR RECOVERY" on the top of the CHP-180 as well as use the stat "835" as a secondary MDT Log Clearance.

Plate scan information is retained for a period of two years and may be queried for use in law enforcement investigations. Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law

enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a "vehicle of interest" is located. Current use of hot lists include AMBER alerts and vehicles associated with 290 sex registrants. Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information entered by SCC personnel, hot list information intended for Department-wide use must have the approval of the Director of the Law Enforcement Information Sharing Program. Mobile ALPR users can input individual license plates into their patrol vehicle's ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a "vehicle of interest" which is not necessarily wanted for a crime (ex: sex registrants vehicle). Personnel must use discretion and in some cases have independent information justifying a traffic stop.

Questions regarding the use of ALPR equipment or accessing plate scan information may be directed to the Advanced Surveillance and Protection Unit at

Questions regarding the content of this Field Operations Directive may be directed to Field Operations Support Services at

### Affected Directives/Publication

Manual of Policy and Procedures §5-09/210.00 Pursuits

### Cites/References

<http://www.pipstechnology.com/>

DRB:WJM:TPA:CWR:NBT:WJM:JLS:EPF:ef

# **Exhibit B**

September 5, 2012

Ms. Lynch,

## **AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM**

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles, as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists". The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database six times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) or Mobile Digital Computer (MDC), prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server within seconds of the scans occurring. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Most mobile ALPR units do not have a "continuous" connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at the beginning and end of their shift to ensure they have the latest informational data available. If the ALPR system is integrated with an MDC, it is possible for the user to update their data via the unit's cellular connection in the field.

### **BOSS (Back Office System Server)**

The BOSS server is where all the stored ALPR data resides. Within the server are the "hotlists," which are deployed and used to compare the license plates that are scanned by the ALPR cameras. The "hotlists" are maintained by the ASAP (Advanced Surveillance and Protection) Unit and are set-up to refresh automatically. There are a few cases which specific hotlists have been set-up for certain units and they have to be updated manually (most of these lists are covert hotlists and the user is not notified of the "hit"). The primary use of the server is for storage of the license plate data captured. Currently, we maintain approx. (2) years' worth of license plate data from all of our LASD ALPR cameras. Detectives and other investigative resources can utilize the BOSS database in searches for full or partial license plate information. Additionally, we have set-up links to query other LA County police agencies approx. 26 at this time, and are in the process of setting up and expanded ability to search other county law enforcement agencies with ALPR such as San Bernardino County Sheriff and Riverside County Sheriff.

## **Department Policies and Guidelines**

There are no written guidelines as to how to use the data. The policy of how we use Department resources (data) is listed below. Keep in mind data is often used as a "lead" to glean further information on an active investigation that law enforcement handles.

Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

### **3-07/200.00 SHERIFF'S DATA NETWORK (SDN)**

The Sheriff's Data Network (SDN) central hub is at the Sheriff's Headquarters Building and is under the administration of Data Systems Bureau.

The Sheriff's Data Network is a high speed network connecting all Sheriff's Department facilities and participating Los Angeles County municipal police departments. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, LA Net, CLETS, and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJIS, LARCIS, CWS, CCHRS, RAPS, FMS, Cal Gangs (Formerly GREAT), CWTAPPS, JDIC and the Department's Intranet Server. For an up-to-date list of applications available on the Sheriff's Data Network, contact the Data Systems Bureau Help Desk.

### **3-07/210.00 PERMISSIBLE USE**

The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

### **3-07/220.00 PROHIBITIONS**

Employees shall not add, alter, copy, damage, delete, move, modify, tamper with or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- Devise or execute any scheme or artifice to defraud, deceive, destroy or extort,
- Wrongfully control or obtain money, property, or data,
- Disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network,
- Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

Unless specifically authorized by Data Systems Bureau, Department employees shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software.

#### **Employees shall not do any of the following without the required authorization:**

- Access or allow access to another to obtain, alter, or prevent access to stored electronic communications,
- Use electronic communications to capture or open electronic communications of another, or access files without permission of the owner,
- Damage hardware, software, or other communications equipment or interfere with functionality,
- Attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission,
- Modify or delete any file, folder or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records,
- Access the files belonging to another for non-business purposes,
- Use someone else's USERID, password or access another person's files, or retrieve stored communications without authorization,
- Modify the hardware or software configuration on any computer,
- Use electronic communications to transmit (upload) or receive (download):
  - Any communication violating any applicable laws, regulations, or policies,
  - Proprietary or confidential Department information,
  - Chain letters,
  - Material that would be offensive to a reasonable person.
- Transmit any electronic message in violation of file size restrictions,
- Use Department computer equipment or network to send or receive electronic communications for non-Department business,
- Use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the County or third parties,



- Send or receive commercial software in violation of its license agreement,
- Copy personal files, programs, or images into any Department computer without authorization from their unit commander,
- Send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual or contain derogatory racial or religious content,
- Establish any hidden or misidentified links on any web page,
- Send or forward messages which have been altered in order to deceive the receiver as to the original content,
- Use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use,
- Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment,
- Use electronic communications in competition with commercial services to individuals or organizations outside the Department,
- Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering,
- Give out employee personal information such as home address and/or telephone numbers.

### **3-07/220.20 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT**

- As an employee of the Los Angeles County Sheriff's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 - 11144 and 13301 - 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:
- "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."
- California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any employee who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

**3-07/250.00 LASD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES**

Employees will be responsible for reading and signing the Sheriff's Department "User Acknowledgment of Electronic Communications Policy" form before obtaining authorization to access the Sheriff's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of sergeant or higher. An employee may request authorization to access the Sheriff's Data Network by submitting the request as described under the manual section entitled, Data Communications Management (section 3-07/230.00), and attaching the signed user acknowledgment form.

**User Acknowledgment of Electronic Communications Policy**

---

I understand that the Los Angeles County Sheriff's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures, section 3-07/200.10 through section 3-07/250.00 inclusive. I have received a copy of these sections of the Manual of Policy and Procedures.

I understand that I must not have an expectation of privacy when using County electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized employees.

By signing this form, I agree to abide by all policies, including state statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions, and that disciplinary actions may result from not abiding by these policies. I also agree to give authorized persons, including supervisors, auditors, and investigators access to my equipment, software, and files at reasonable times for the purposes of investigating compliance.

---

User Name (PRINT)  
Date

User Signature

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, section 3-07/200.10 through section 3-07/250.00 inclusive, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands' this policy.

---

Supervisor's Name (PRINT)  
Date

Supervisor's Signature

\* Attached is our Field Operations Directive as to how we utilize ALPR in the field \*

We do not have user manuals for members of the Department. We train personnel in groups utilizing the train the trainer methodology. Both interfaces of the ALPR system are intuitive and do not require extensive training.

Retention is currently limited by the size of the data stored. As we expand the number of ALPR units, we additionally have to minimize the retention of the data we keep. Currently, we would prefer to retain data indefinitely but this will change if we cannot keep up with the increasing data storage requirements. There is no national or state mandate specifically for ALPR data retention (in California) and we have looked at similar standards, such as video, which is currently (2) years.

Sergeant John Gaw  
LASD / Technical Services Division  
Communications and Fleet Management Bureau (CFMB)  
Advanced Surveillance and Protection Unit (ASAP)  
12440 East Imperial Highway, #130  
Norwalk, CA 90650  
(562) 345-4476 / Office  
[jl Gaw@lasd.org](mailto:jl Gaw@lasd.org)  
[asap@lasd.org](mailto:asap@lasd.org)  
<http://intranet.lasd.sheriff.sdn/intranet/announcements/ASAP/ASAP.shtml>  
[www.comptonasap.com](http://www.comptonasap.com)  
<http://www.lasd.org/sites/ASAP/index.html>  
<http://www.youtube.com/user/LACountySheriff>



**ASAP**

ADVANCED SURVEILLANCE AND PROTECTION



# ***Los Angeles County Sheriff's Department***

## ***Automatic License Plate Recognition-ALPR***

*Deployed on radio cars*



*or at fixed locations*

## ***Automatic License Plate Recognition Cameras***

***3 camera assemblies located on  
radio light bar***

---



***Each camera assembly contains a  
color camera and an infrared  
camera***

---



# Mobile ALPR

*Deputies view of monitor*





# *Fixed Cameras in Compton*





*The original concept of License Plate Recognition was to identify stolen vehicles. Since it's deployment, additional applications have been implemented and continue to develop,*

## Benefits of ALPR/BOSS

- ALPR has the "ability" to read more than 14,000 license plates during the course of a shift (does not read black or blue),
- can read a license plate, coming in the opposite direction, at over 160mph (closing speed)
- provides an overview photograph of the vehicle and its license plate,
- imbeds a "stamp" of the date, time, GPS coordinates, and other data,
- can also obtain the license plate in difficult conditions. For example, poor lighting conditions, or when the vehicle is approaching and it's headlights make it difficult to read.



## Applications for ALPR

- locate wanted/stolen vehicles,
- identify vehicles with L.A. County misdemeanor warrants of \$26,000 or greater, all felony warrants, and no bail warrants,
- locate vehicles identified by the Amber alert system,
- locate vehicles which are frequently sold or not registered,
- assist in traffic enforcement by identifying drivers with outstanding DUI's, suspended license warrants. which frequently result in higher hit and runs collisions,
- monitor "party calls" where assaults and homicides sometimes occur, providing critical investigative information,
- monitor locations of suspected narcotic or gang activity,
- monitor motels where criminals may attempt to hide and evade law enforcement, or large parking lots,

*-provide data for department investigators to search areas impacted by rising crime rate such as residential burglaries, vehicle burglaries and thefts,*

*-provide data where station desk personnel can access license plate information related to, "just occurred" calls. That information can be provided to responding units where detailed vehicle information can be updated from photographs in the BOSS system, extremely useful to Sheriff department Area units, possible direction of travel or destinations can be provided, follow vehicles may be identified,*

*- additional victims and witnesses may be identified. Investigators have deployed ALPR in locations where a crime has occurred, identified motorists who commute in that area during that time period,*

*- it may also be useful in clearing someone of an allegation and help determine the truthfulness of a suspect or witness,*

## Brief overview of an ALPR car

*Deputies will download the updated wanted/stolen information via a wireless connection at their station,*



*During or at the end of their shift, they can upload their scans/reads to the BOSS server which will now be available to department investigators,*





**Important considerations regarding access to the data;**

*The Department of Justice (DOJ) provides updated lists of stolen/wanted vehicles 3 times a day,*

*2:45 AM*

*10:45 AM*

*6:45 PM*

*Warrant information is updated 2 times a day,*

*Scans or reads are stored in the processor located in the trunk, until the deputy uploads the data at the station to the server,*

*Patrol deputies have the ability to manually enter license plates into their ALPR system, (i.e a 215 P.C. just occurred),*

# How to access the BOSS system

Internet Policy - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://intranet/intranet/sites/DSB/InternetUsePolicy.htm>

Google Search

Internet User Guidelines...

INTRANET INTERNET LASD.ORG

CLICK HERE FOR DETAIL INFORMATION ON:  
**DATA SECURITY POLICIES**

**INTRODUCTION:**  
*As the Sheriff Department expands its technology offerings and makes Internet access available to all users, it is important to keep Department guidelines in mind when it comes to using computers and the Internet. For this reason your Internet Explorer default has been set to this web page listing the Internet Use Guidelines.*

**MPP 3-07/210.00 PERMISSIBLE USE:**  
*The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.*

*Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.*

**GUIDELINES:**  
*Managing each user's Internet access will be the responsibility of the unit where the user is assigned.  
A Unit Commander at his/her discretion may allow, restrict or remove Internet access for any user in their unit.  
LASD will filter access to Internet sites and Internet usage in general. Web sites, Web services, or materials deemed inappropriate by the Department will be blocked and not made available to users.  
All uses of LASD's Internet access service which are in violation of any federal, state or local law, County of Los Angeles Code, LASD's Policy and Procedures Manual, or these guidelines are strictly prohibited.  
All Internet access through the Sheriff's Data Network is monitored and logged on an ongoing basis. LASD has the right and capability to monitor Internet usage by each user on the system.*

Done Local intranet

start | Inbox - Microsoft Out... | BOSS - Back Office S... | aot powerpoint-BOSS | CTT/Plus - [SRC CAD] | Internet Policy - Mic... | Search with Google | 4:03 PM

Los Angeles County Sheriff's Department Home page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address: https://intranet/intranet/index.html

Google

Go 12 blocked Check Look for Map Send to Settings



**In Memoriam**  
 The Los Angeles County Sheriff's Department - Santa Clarita Valley Station is saddened to announce the loss of one of its deputies. After a long and hard fought battle, Deputy Randy Hanson succumbed to injuries he sustained after being struck by a car on Saturday, August 16, 2004.

Global Search Search by Category

Home General Info Administration Organizational Library News & Highlights Web Applications Business Services Tech Support/Services Other Links

**What's New ?**  
 This site provides information on various development efforts underway or exploration of new technologies for adoption throughout the department.  
**ISSUE NO. 17** **SEPTEMBER 2008**  
**TECH TIPS**  
 Sheriff's Communications Center better known as SCC is one of the largest and most complex communications systems in the entire nation - Read more about its evolution - 50 years and a world of difference! [SCC: then and now](#)

**Crime Scene 3-D Laser Scanner . .**  
**SEE IT IN ACTION!**  
**ASAP**  
ADVANCED SURVEILLANCE AND PROTECTION

**Sheriff's Corner**  
 Leadership Message from the Sheriff  
 This is a new series of articles written by the Sheriff himself which will incorporate our Core Values and Department Creed, as we utilize them in the performance of our duties.

**Build a structure around a vision**

**LASER Achievements**  
 "To memorialize and celebrate our time and effort, I have highlighted some of our major achievements over the past four years to celebrate and acknowledge our endeavors..."

**Public Trust Policing**  
 Sheriff's Philosophy on Public Trust

Done Local Intranet

start Intranet - Microsoft Out... CTT/Bus - [SPC CAP] Detective presentation Los Angeles County S... Search with Google 10:33 AM

Advanced Surveillance and Protection - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://intranet.lacd.sheriff.ad/intranet/announcements/ASAP/ASAP.shtml

Google

# ASAP

ADVANCED SURVEILLANCE AND PROTECTION

- Back to LAMP Intranet
- ASAP Home
- Integrated Technologies
- Compton ASAP Pilot
- Compton Project Phases
- Contact Us



## ASAP TOOLS

- License Plate Recognition Search Engine
- ASAP Deployment
- ASAP Tutorials
- ASAP News
- ASAP Success Stories

### ADVANCED SURVEILLANCE AND PROTECTION - ASAP

The Los Angeles County Sheriff's Department enjoys a reputation of leadership and excellence in law enforcement tactics, training, and technology. Consistent with that reputation, our Department is piloting the Advanced Surveillance and Protection (ASAP) plan to assist with our gang and crime fighting efforts.

ASAP features a variety of technologies such as high-definition digital video surveillance, audio/golfball detection, automatic license plate recognition (ALPR), and other advanced vehicle components, integrated into a command center functioning with station dispatch. Some of the technical components have already been used by the Sheriff's Department and throughout the county for limited law enforcement applications. ASAP will serve to expand the use of advanced technologies in the field, strengthen criminal procedures with video evidence, and provide real-time intelligence to improve officer safety.

The ASAP pilot will be deployed at Compton Station, with the initial phases of Compton ASAP being funded through the generous support of corporate partners such as Baker and Taylor Corporation.

The Sheriff's Technical Services Division is establishing the best practices and coordinating deployment throughout the Department. Many of our contact sites are already working with the Sheriff's Department to develop a strategy to deploy ASAP at some of its components within their communities.

For information on ASAP, contact the word unit at (924) 241-4200 or email [word@lacsd.net](mailto:word@lacsd.net)

Internet

start | Inco - Microsoft Out... | Microsoft PowerPoint... | Lac Angeles County S... | Advanced Surveill... | Search with Google | 1:24 PM

# ASAP TOOLS



License Plate Recognition  
Search Engine



ASAP Deployment



ASAP Tutorials



ASAP News



ASAP Success Stories

Log in screen

**BOSS: BACK OFFICE SYSTEM SERVER** COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

Done Local intranet

start | Inbox - Microsoft Out... | CTT/Plus - [SRC CAD] | Detective presentation | Los Angeles County S... | BOSS - Back Office S... | Search with Google | 10:32 AM

***LOGIN NAME:***

***PASSWORD:***

Logon

**[FORGOT YOUR LOGIN NAME OR PASSWORD?](#)**

BOSS - Back Office System Server - Windows Internet Explorer

http://4-icn-olp-web:8080/BOSS/GUI/FormaDefault/Default.aspx

File Edit View Favorites Tools Help

Google Search

BOSS - Back Office System Server

Home Pages Print Page Tools

**piPS** **BOSS** 47N R3A

**HELLO HOMICIDE BUREAU, WELCOME TO BOSS.**

**READS**  
7924264

**HITS**  
15430

**MISDEMEANOR**  
255

**Audit Inves**  
48789

**TARGETS**  
0

**BOSS STATE (INCLUDE ALL ARCHIVES)**

**BOSS: Back Office System Server** **COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.**

Connected to BOSS dispatch. Local Intranet 100%

Inbox - Microsoft Outlook BOSS - Back Office System Server 8:40 PM



HOME

REPORTS

ADMIN

SYSTEM

PIPS

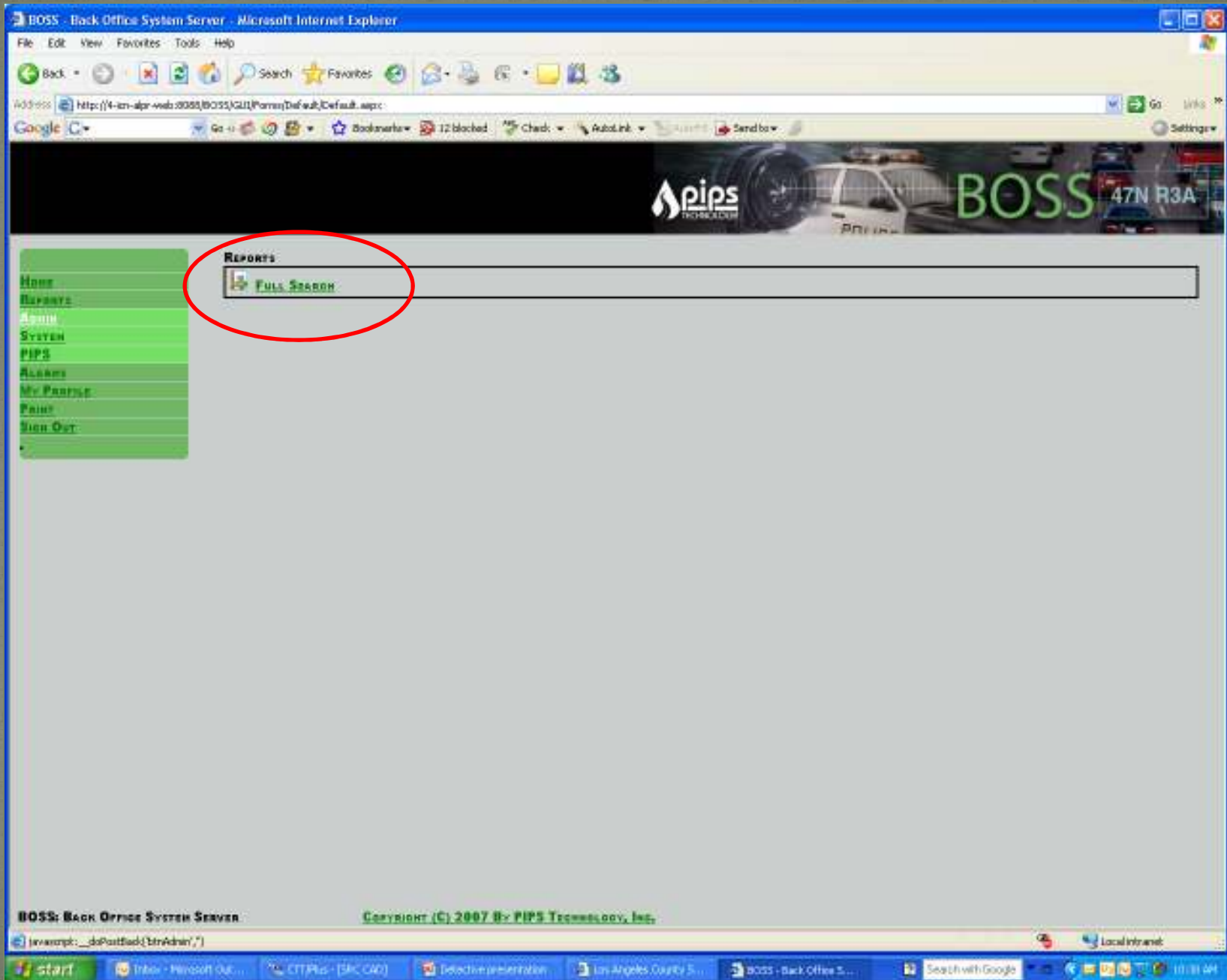
ALARMS

MY PROFILE

PRINT

SIGN OUT

▪



# Search screen



- HOME
- REPORTS
- ADMIN
- SYSTEM
- PIPS
- ALARMS
- MY PROFILE
- PRINT
- SIGN OUT

NEW SEARCH

LICENSE PLATE

LOGIN

LOCATION

INFORMATION

ADDRESS

RADIUS

MI  KM

OPTIONS

MISREADS ONLY

HITS ONLY

No PAGING

FROM ARCHIVED DATA

START DATE AND TIME

30 Apr 2009 12 48

SERVERS

END DATE AND TIME

30 Jul 2009 12 48

- Local
- All Servers
- Long Beach PD
- El Segundo PD
- Burbank PD
- La Verne PD
- Monrovia PD
- Glendora PD
- Torrance PD
- CSU Long Beach PD
- Irwindale PD
- Arcadia PD
- South Pasadena PD
- San Gabriel PD
- Glendale PD
- Beverly Hills PD
- Monterey Park PD
- Sierra Madre PD
- Gardena PD
- Vernon PD
- Hawthorne PD

Local ← All lasd vehicles/sights

All Servers ←

Long Beach PD

El Segundo PD

Burbank PD

La Verne PD

Monrovia PD

Glendora PD

Torrance PD

CSU Long Beach PD

Irwindale PD

Arcadia PD

South Pasadena PD

San Gabriel PD

Glendale PD

Beverly Hills PD

Monterey Park PD

Sierra Madre PD

Gardena PD

Vernon PD

Hawthorne PD

LAPD

Manhattan Beach PD

Pasadena PD

South Gate PD

Search

# Outside Agency Servers

The screenshot displays the BOSS (Back Office System Server) interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL: `http://4-az-als-web:8080/BOSS/GUI/Power/Default/Default.aspx`. The page features a navigation menu on the left with options like Home, Reports, Admin, SYSTEM, PIPS, Alarms, My Profile, Print, and Sign Out. The main content area is titled "SEARCH RESULTS" and contains two sections for search results.

The first section is for "ARCADIA PD SERVER RESULT SET" and shows "EVENTS(1)". It includes a table with the following data:

VLP	TIMESTAMP	OVERVIEW	PATH	INFORMATION	LOGIN
<a href="#">SELECT</a>	6/27/2009 1:38:03 AM				241

The second section is for "SOUTH PASADENA PD SERVER RESULT SET" and also shows "EVENTS(1)". It includes a table with the following data:

VLP	TIMESTAMP	OVERVIEW	PATH	INFORMATION	LOGIN
<a href="#">SELECT</a>	7/13/2009 2:50:14 PM				0803

The footer of the page contains the text: "BOSS: BACK OFFICE SYSTEM SERVER" and "COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.". The Windows taskbar at the bottom shows the Start button, open applications, and the system tray with the time 5:34 AM.

Searching a license plate,

NEW SEARCH

LICENSE PLATE

1ABC123

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28 ▼ Sep ▼ 2008 ▼

13 ▼ 42 ▼

END DATE AND TIME

26 ▼ Oct ▼ 2009 ▼

13 ▼ 42 ▼

Searching a partial license plate,

NEW SEARCH

LICENSE PLATE

1ABC\*

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28 Sep 2008

13 42

END DATE AND TIME

26 Oct 2009

13 42

1ABC\*

\*C123

\*ABC\*

1AB\_123

1A\_C1\_3

\*ABC\_\_3

Searching by an LASD/ALPR vehicle

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28	▼	Sep	▼	2008	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---

END DATE AND TIME

26	▼	Oct	▼	2009	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---





## Searching by date(s)

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28 ▼ Sep ▼ 2008 ▼ 13 ▼ 42 ▼

END DATE AND TIME

26 ▼ Oct ▼ 2009 ▼ 13 ▼ 42 ▼

and times,

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28 ▼ Sep ▼ 2008 ▼

13 ▼ 42 ▼

END DATE AND TIME

26 ▼ Oct ▼ 2009 ▼

13 ▼ 42 ▼

*Search by station*

LOGIN

CAS

INFORMATION

MI  KM

No PAGING

FROM ARCHIVED DATA

SERVERS

Local

*Search beyond 45 days*

Date and time

Vehicle photo

		Date and time	Vehicle photo	License plate	Description	Category
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 12:13:14 PM		4X0Y215	LACO WARRANT: LAM9MP0705901, 23152(A)/VC MISDEMEANOR,	VES-34
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 11:47:44 AM		6RTK715	STOLEN VEHICLE: CA1920090608	VES-14
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 11:22:05 AM		3L2H558	LOST OR STOLEN PLATE: CA1920070330	VES-29
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 11:13:14 AM		66F1279	LOST OR STOLEN PLATE: CA1920090105	VES-33
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 10:23:36 AM		570C130	LACO WARRANT: P49854919000, 12500A/VC MISDEMEANOR,	PLM
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 10:22:53 AM		570C130	LACO WARRANT: P49854919000, 12500A/VC MISDEMEANOR,	PLM
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 9:33:38 AM		7533665	LACO WARRANT: LC7BF0568501, 14601.1(A)/VC MISDEMEANOR,	GEN
<a href="#">SELECT</a>	[REDACTED]	7/30/2009 8:55:08 AM		[REDACTED]	LOST OR STOLEN PLATE: CA5420080905	GEN

BOSS: BACK OFFICE SYSTEM SERVER

COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

Both license plates

**You MUST compare these plates. All hits must be confirmed.**

**If they do not match, it did not check the data base correctly, but the scanned plate may still be identifiable.**

GPS map

File Edit View Favorites Tools Help

Address: http://14-101-101-101:8080/BOSS/Forms/Default.aspx

Google Search

**pips** BOSS 47N R3A

TIME STAMP: 7/30/2005 10:28:00 AM

LOCATION: PLM-M-SD7000

GPS: 34.601925, -118.14427

LACO Warrant	[REDACTED]	\$60,035.00	P49854919000, 12500A/VC MISDEMEANOR,
--------------	------------	-------------	--------------------------------------

MAP SATELLITE HYBRID

BOSS: BACK OFFICE SYSTEM SERVER

Copyright (C) 2007 By PIPS Technology, Inc.

# Satellite view

File Edit View Favorites Tools Help

Back Search Favorites

Address: http://4-tn-apt-web:8088/BOSS/GOI/Forms/Default/Default.aspx

Google Search Bookmarks Check AutoFill

**pips** TECHNOLOGIES **BOSS** 47N R3A

TIME STAMP: 11/30/2009 10:24:50 AM

LOCATION: PLM-M-SD7000

GPS: 34.601925, -118.14427

LACD Warrant		\$60,035.00	P49854919000, 12500A/VC MISDEMEANOR,
--------------	--	-------------	--------------------------------------

MAP **SATellite** HYBRID

BOSS: BACK OFFICE SYSTEM SERVER

Copyright (C) 2007 by PIPS Technology, Inc.



*Deputies in the cars can enter license plates they wish to search for. An example might be a 215 P.C. just occurred.*




















*An investigator can also request the field deputy to enter a plate that they are trying to locate.*

*The advantage to a manual entry is that the car's ALPR system is updated immediately and you do not have to wait for the deputy to update at the station through the wireless connection.*

*Once the field deputy conducts the wireless update, the manual entry is deleted from the radio car and entered into BOSS. It does not update the other vehicles that the vehicle is wanted.*

*A manual entry in BOSS may look like a scan, but it is not. The difference is that there is no photograph of the scan, the "confidence" number is "100", and the location will be the GPS where the entry was made, (i.e. a Sheriff's station).*

*A Century deputy manually entered a stolen vehicle they were looking for,*

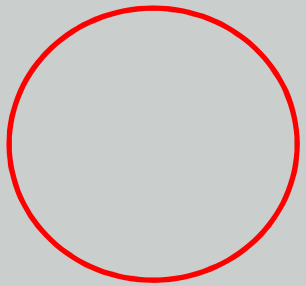
		 	
<a href="#">SELECT</a>	5769444 [REDACTED]	6:42:58 AM	  LACO WARRANT: PAS8PS6811301, 12500(A)/VC MISDEMEANOR, CVS
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:42:58 AM	  LACO WARRANT: PAS8PS6811301, 12500(A)/VC MISDEMEANOR, CVS
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:38:13 AM	  LOST OR STOLEN PLATE: CA3020070216 ELA
<a href="#">SELECT</a>	5 [REDACTED]	7/29/2009 6:35:52 AM	  LACO WARRANT: 911916719420, 146011A/VC INFRACTION, LNX
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:20:58 AM	 STOLEN VEHICLE: CA1920090729 GEN
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:11:37 AM	  LACO WARRANT: COM9CP0154101, 14601.1(A)/VC MISDEMEANOR, GEN
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:10:16 AM	  LACO WARRANT: COM9CP0154101, 14601.1(A)/VC MISDEMEANOR, GEN
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:05:02 AM	  STOLEN VEHICLE: CA1920090726 LNX
<a href="#">SELECT</a>	[REDACTED]	7/29/2009 6:03:48 AM	  STOLEN VEHICLE: CA1920090726 LNX

IVER

COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

No vehicle photo

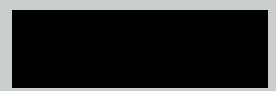
"Confidence" level is "100"



LOGIN ID: CEN  
CONFIDENCE: 100

TIMESTAMP: 7/29/2009 6:20:58 AM

LOCATION: CEN-M-SD5837



GPS: 33.95564, -118.253298333333

Stolen Vehicle	5SOH313						CA1920090729
----------------	---------	--	--	--	--	--	--------------



# Export Function

Each results page will have an "Export" function link. This will export all relative information from the results page. This can then be entered into an Excel spreadsheet, WORD document, etc

BOSS - Back Office System Server - Microsoft Internet Explorer

Address: http://146.233.6.211:8088/BOSS/GUI/Forms/Default/Default.aspx

BOSS 47N R3A

2007-05-21 8:59:59 PM

HOME  
REPORTS  
FULL SEARCH  
AUDIT HISTORY  
ADMIN  
SYSTEM  
PIPS  
ALARMS  
MY PROFILE  
PRINT  
SIGN OUT

SEARCH RESULTS

LOCAL SERVER RESULT SET

EVENTS(31) . EXPORT

MAX RESULTS: 1000

	VLP	TIMESTAMP	OVERVIEW	PATCH	INFORMATION
<a href="#">SELECT</a>		2007-04-18 12:50:54 PM			
<a href="#">SELECT</a>		2007-04-18 5:37:22 PM			
<a href="#">SELECT</a>		2007-04-19 12:29:07 AM			
<a href="#">SELECT</a>		2007-04-21 12:23:29 AM			

BOSS: BACK OFFICE SYSTEM SERVER COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

# Export Function

Displays all information for each vehicle in results. Displays the following: Read ID, Vehicle login, Confidence, Timestamp, GPS location, etc.

BOSS - Back Office System Server - Microsoft Internet Explorer

Address: http://146.233.6.211:8088/BOSS/GUI/Forms/Default/Default.aspx

BOSS 47N R3A

2007-05-24 8:31:53 AM

Read\_id, Vrm, Login\_id, Confidence, Timestamp, Syntax, Location, Latitude, Longitude, Xaxis, Yaxis, Zaxis, M1a

"15687"	"5HQ2563"	"12", "98"	"2007-04-18 1:03:06 AM"	"", "CPT"	"33.9167666666667"	"-118.2080533333333"						
"15692"	"5HQ2563"	"12", "97"	"2007-04-18 1:03:41 AM"	"", "CPT"	"33.9167633333333"	"-118.2080483333333"						
"21818"	"5GS1849"	"12", "92"	"2007-04-18 6:36:28 PM"	"", "CPT"	"33.912195"	"-118.21686"	"-0.39238206"					
"21818"	"5GS1849"	"12", "92"	"2007-04-18 6:36:28 PM"	"", "CPT"	"33.912195"	"-118.21686"	"-0.39238206"					
"23104"	"5VPU722"	"12", "98"	"2007-04-18 9:10:24 PM"	"", "CPT"	"33.9032533333333"	"-118.2203666666667"						
"23106"	"5VPU722"	"12", "96"	"2007-04-18 9:10:37 PM"	"", "CPT"	"33.9032383333333"	"-118.2203833333333"						
"23109"	"5VPU722"	"12", "97"	"2007-04-18 9:12:07 PM"	"", "CPT"	"33.903155"	"-118.22039"	"-0.39246871"					
"23111"	"5VPU722"	"12", "96"	"2007-04-18 9:12:17 PM"	"", "CPT"	"33.9032433333333"	"-118.2203833333333"						
"23112"	"5VPU722"	"12", "100"	"2007-04-18 8:12:47 PM"	"", "CPT"	"33.9032366666667"	"-118.2203583333333"						
"23114"	"5VPU722"	"12", "90"	"2007-04-18 9:13:41 PM"	"", "CPT"	"33.9032366666667"	"-118.22041"	"-0.39246871"					
"23114"	"5VPU722"	"12", "90"	"2007-04-18 9:13:41 PM"	"", "CPT"	"33.9032366666667"	"-118.22041"	"-0.39246871"					
"23595"	"5XXY921"	"12", "97"	"2007-04-18 10:53:50 PM"	"", "CPT"	"33.8943983333333"	"-118.2286316666666"						
"23800"	"5FHL832"	"12", "97"	"2007-04-19 12:43:08 AM"	"", "CPT"	"33.8858233333333"	"-118.2693133333333"						
"25354"	"5VPU722"	"12", "100"	"2007-04-19 12:51:09 AM"	"", "CPT"	"33.902965"	"-118.220445"	"-0.39246871"					
"25354"	"5VPU722"	"12", "100"	"2007-04-19 12:51:09 AM"	"", "CPT"	"33.902965"	"-118.220445"	"-0.39246871"					
"25356"	"5VPU722"	"12", "97"	"2007-04-19 2:16:07 AM"	"", "CPT"	"33.9030933333333"	"-118.220475"	"-0.39246871"					
"25356"	"5VPU722"	"12", "97"	"2007-04-19 2:16:07 AM"	"", "CPT"	"33.9030933333333"	"-118.220475"	"-0.39246871"					
"25378"	"1HBN944"	"12", "100"	"2007-04-19 1:35:07 AM"	"", "CPT"	"33.90144"	"-118.22064"	"-0.39247979"					
"25378"	"1HBN944"	"12", "100"	"2007-04-19 1:35:07 AM"	"", "CPT"	"33.90144"	"-118.22064"	"-0.39247979"					
"25417"	"5GS1849"	"12", "98"	"2007-04-19 2:44:24 AM"	"", "CPT"	"33.9122383333333"	"-118.2168866666667"						
"25417"	"5GS1849"	"12", "98"	"2007-04-19 2:44:24 AM"	"", "CPT"	"33.9122383333333"	"-118.2168866666667"						
"25433"	"5VPU722"	"12", "98"	"2007-04-19 2:48:35 AM"	"", "CPT"	"33.8988866666667"	"-118.2075783333333"						
"25433"	"5VPU722"	"12", "98"	"2007-04-19 2:48:35 AM"	"", "CPT"	"33.8988866666667"	"-118.2075783333333"						
"25534"	"5VPU722"	"12", "100"	"2007-04-19 2:06:51 AM"	"", "CPT"	"33.9091783333333"	"-118.2115166666666"						
"25534"	"5VPU722"	"12", "100"	"2007-04-19 2:06:51 AM"	"", "CPT"	"33.9091783333333"	"-118.2115166666666"						
"25536"	"5VPU722"	"12", "100"	"2007-04-19 2:08:11 AM"	"", "CPT"	"33.9092283333333"	"-118.2115"	"-0.39246871"					
"25536"	"5VPU722"	"12", "100"	"2007-04-19 2:08:11 AM"	"", "CPT"	"33.9092283333333"	"-118.2115"	"-0.39246871"					
"25791"	"7L00245"	"12", "100"	"2007-04-19 3:38:06 AM"	"", "CPT"	"33.8959683333333"	"-118.20464"	"-0.39246871"					
"27123"	"5SL1155"	"12", "98"	"2007-04-19 9:41:20 PM"	"", "CPT"	"33.9111666666667"	"-118.212265"	"-0.39246871"					

BOSS: BACK OFFICE SYSTEM SERVER COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

# Export Data Pasted into Excel

ALPR data pasted in Excel can be modified and searched for crime analysis

The screenshot shows a Microsoft Excel spreadsheet titled "Hits.xls" with a table of ALPR data. The table has 12 columns and 28 rows of data. The columns are: Read\_id, Vrm, Login\_id, Confidence, Timestamp, Location, Latitude, Longitude, Xaxis, Yaxis, Zaxis, and Misread. The data includes vehicle identification numbers (Vrm), license plate numbers (Login\_id), confidence scores, timestamps, locations (CPT), and geographic coordinates (Latitude, Longitude, Xaxis, Yaxis, Zaxis). The Misread column contains the value "FALSE" for all entries.

	A	B	C	D	E	G	H	I	J	K	L	M
	Read_id	Vrm	Login_id	Confidence	Timestamp	Location	Latitude	Longitude	Xaxis	Yaxis	Zaxis	Misread
1	15687	5HQZ563	12	98	4/18/2007 1:03	CPT	33.91676657	-118.2080533	-0.392248588	-0.731293693	0.557987975	FALSE
2	15692	5HQZ563	12	97	4/18/2007 1:03	CPT	33.91676333	-118.2080483	-0.39224854	-0.731293756	0.557987926	FALSE
3	21818	5GSAB49	12	92	4/18/2007 18:36	CPT	33.912195	-118.21686	-0.392382037	-0.731272623	0.557921759	FALSE
4	21818	5GSAB49	12	92	4/18/2007 18:36	CPT	33.912195	-118.21686	-0.392382037	-0.731272623	0.557921759	FALSE
5	23104	5VPU722	12	98	4/18/2007 21:10	CPT	33.90325333	-118.2203667	-0.39246796	-0.731325318	0.557792237	FALSE
6	23106	5VPU722	12	96	4/18/2007 21:10	CPT	33.90323833	-118.2203833	-0.392468241	-0.731325332	0.55779202	FALSE
7	23109	5VPU722	12	97	4/18/2007 21:12	CPT	33.903155	-118.22039	-0.39246871	-0.731326002	0.557790813	FALSE
8	23111	5VPU722	12	96	4/18/2007 21:12	CPT	33.90324333	-118.2203833	-0.392468218	-0.73132529	0.557792092	FALSE
9	23112	5VPU722	12	100	4/18/2007 20:12	CPT	33.90323667	-118.2203583	-0.39246793	-0.731325518	0.557791996	FALSE
10	23114	5VPU722	12	90	4/18/2007 21:13	CPT	33.90323667	-118.22041	-0.39246859	-0.731325164	0.557791996	FALSE
11	23114	5VPU722	12	90	4/18/2007 21:13	CPT	33.90323667	-118.22041	-0.39246859	-0.731325164	0.557791996	FALSE
12	23695	5XY921	12	97	4/18/2007 22:53	CPT	33.89439833	-118.2286317	-0.39261422	-0.731344641	0.557663958	FALSE
13	23800	5FMLB32	12	97	4/19/2007 0:43	CPT	33.88582333	-118.2693133	-0.393172922	-0.731139188	0.557539722	FALSE
14	25354	5VPU722	12	100	4/19/2007 0:51	CPT	33.902965	-118.220445	-0.392470287	-0.731327255	0.557788061	FALSE
15	25354	5VPU722	12	100	4/19/2007 0:51	CPT	33.902965	-118.220445	-0.392470287	-0.731327255	0.557788061	FALSE
16	25356	5VPU722	12	97	4/19/2007 2:16	CPT	33.90309333	-118.220475	-0.392470079	-0.731325948	0.55778992	FALSE
17	25356	5VPU722	12	97	4/19/2007 2:16	CPT	33.90309333	-118.220475	-0.392470079	-0.731325948	0.55778992	FALSE
18	25378	1HBN944	12	100	4/19/2007 1:35	CPT	33.90144	-118.22064	-0.392479796	-0.731339	0.557765969	FALSE
19	25378	1HBN944	12	100	4/19/2007 1:35	CPT	33.90144	-118.22064	-0.392479796	-0.731339	0.557765969	FALSE
20	25417	5GSAB49	12	98	4/19/2007 2:44	CPT	33.91223833	-118.2168867	-0.392382178	-0.731272068	0.557922386	FALSE
21	25417	5GSAB49	12	98	4/19/2007 2:44	CPT	33.91223833	-118.2168867	-0.392382178	-0.731272068	0.557922386	FALSE
22	25433	5VPU722	12	98	4/19/2007 2:48	CPT	33.89888667	-118.2075783	-0.392324812	-0.731450358	0.557728981	FALSE
23	25433	5VPU722	12	98	4/19/2007 2:48	CPT	33.89888667	-118.2075783	-0.392324812	-0.731450358	0.557728981	FALSE
24	25534	5VPU722	12	100	4/19/2007 2:06	CPT	33.90917833	-118.2115167	-0.392327723	-0.731335097	0.557878063	FALSE
25	25534	5VPU722	12	100	4/19/2007 2:06	CPT	33.90917833	-118.2115167	-0.392327723	-0.731335097	0.557878063	FALSE
26	25634	5VPU722	12	100	4/19/2007 2:08	CPT	33.90922833	-118.2115	-0.392327281	-0.731334782	0.557878788	FALSE
27	25634	5VPU722	12	100	4/19/2007 2:08	CPT	33.90922833	-118.2115	-0.392327281	-0.731334782	0.557878788	FALSE
28	25636	5VPU722	12	100	4/19/2007 2:08	CPT	33.90922833	-118.2115	-0.392327281	-0.731334782	0.557878788	FALSE

*The following stat codes are available for ASAP/ALPR;*

*835-ASAP/ALPR-Mobile*

*836-ASAP/ALPR-Fixed*

*837-ASAP-CCTV*

*838-Gunshot detection*

*839-ASAP-misc*

*These stat codes may not be listed in your books. Please include them where possible. Also, any success stories involving ALPR/BOSS can be forwarded to the [asapteam@lasd.org](mailto:asapteam@lasd.org).*

*Email at: ASAPTEAM@LASD.ORG*

**ASAP**

**ADVANCED SURVEILLANCE AND PROTECTION**

*562) 345-4390*



---

# Los Angeles County Sheriff's Department

## FIELD OPERATIONS DIRECTIVE



Field Operations Support Services, (323) 526-5760

---

FIELD OPERATIONS DIRECTIVE: 09-04

DATE: August 17, 2009

ISSUED FOR: OFFICE OF HOMELAND SECURITY  
FIELD OPERATIONS REGIONS  
DETECTIVE DIVISION  
TECHNICAL SERVICES DIVISION

### **AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM**

#### Purpose

The purpose of this directive is to establish procedural guidelines and responsibilities of personnel and units utilizing the Automated License Plate Recognition (ALPR) system. As with any technical system, adherence to standards and procedures is a key element to the success of the system.

#### Background

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans

Originally Issued: 08-17-09  
Revised:  
Latest Revision:

captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists." The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database three times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

### Policy and Procedures

Units utilizing ALPR technology shall publish unit level policy to govern procedures on ALPR usage as well as the syncing of data between the mobile ALPR units and the ALPR server.

Mobile ALPR unit users receiving an alert that a vehicle is stolen, wanted or has a warrant associated with it shall immediately confirm the status of the vehicle by running the license plate either manually via the MDT/CAD or over the radio via SCC, unless compelling circumstances are present or officer safety issues make it unsafe to do so. In such cases, deputies shall confirm the status of the wanted vehicle as soon as possible. When requesting SCC to confirm the status of an ALPR alert, the deputy shall

advise SCC the request is for an ALPR alert on a vehicle.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a "Code-9" due to an ALPR alert on a stolen vehicle, deputies shall advise SCC they are following a vehicle due to an ALPR stolen vehicle alert (i.e. "142F1 is code 9 on 10-29V ALPR hit") prior to receiving a secondary confirmation by MDT/SCC.

Deputies shall adhere to the Department's pursuit policy as described in the Manual of Policy and Procedures § 5-09/210.00. SCC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via SCC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

Any incident associated with the ALPR system shall be documented using a secondary ALPR statistical code. The statistical code shall go on the classification line of the Incident Report (SH-R-49) and in the MDT clearance. Additionally, any vehicle recovered using the ALPR system shall have "ALPR RECOVERY" written across the top of the CHP-180 and the secondary ALPR statistical clearance code will be entered into the MDT clearance log. ALPR statistical codes cannot be used for the issuance of an URN number, but shall be used as a secondary statistical clearance code.

Please ensure the following stat codes are used:

835 - ASAP - ALPR/MOBILE  
836 - ASAP - ALPR/FIXED CAMERA

Examples:

Personnel making an arrest due to an ALPR alert shall enter "835" or "836" as a secondary statistical clearance code in their MDT Log Clearance and on the Classification line of the SH-R-49 report form.

Personnel recovering a stolen vehicle with no suspect in custody shall write "ALPR-CAR RECOVERY" on the top of the CHP-180 as well as use the stat "835" as a secondary MDT Log Clearance.

Plate scan information is retained for a period of two years and may be queried for use in law enforcement investigations. Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law

enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a "vehicle of interest" is located. Current use of hot lists include AMBER alerts and vehicles associated with 290 sex registrants. Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information entered by SCC personnel, hot list information intended for Department-wide use must have the approval of the Director of the Law Enforcement Information Sharing Program. Mobile ALPR users can input individual license plates into their patrol vehicle's ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a "vehicle of interest" which is not necessarily wanted for a crime (ex: sex registrants vehicle). Personnel must use discretion and in some cases have independent information justifying a traffic stop.

Questions regarding the use of ALPR equipment or accessing plate scan information may be directed to the Advanced Surveillance and Protection Unit at [ASAP-Team@LASD.ORG](mailto:ASAP-Team@LASD.ORG) or (562) 345-4476.

Questions regarding the content of this Field Operations Directive may be directed to Field Operations Support Services at [FOSS@LASD.ORG](mailto:FOSS@LASD.ORG) or (323)526-5760.

### Affected Directives/Publication

Manual of Policy and Procedures §5-09/210.00 Pursuits

### Cites/References

<http://www.pipstechnology.com/>

DRB:WJM:TPA:CWR:NBT:WJM:JLS:EPF:ef

# **Exhibit C**

## PAUL PREVOST - instructions

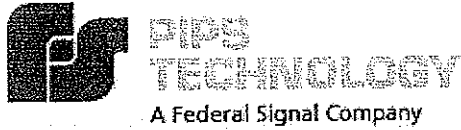
---

**From:** STEPHEN DOLAN  
**To:** PREVOST, PAUL  
**Date:** 10/4/2011 2:58 PM  
**Subject:** instructions

---

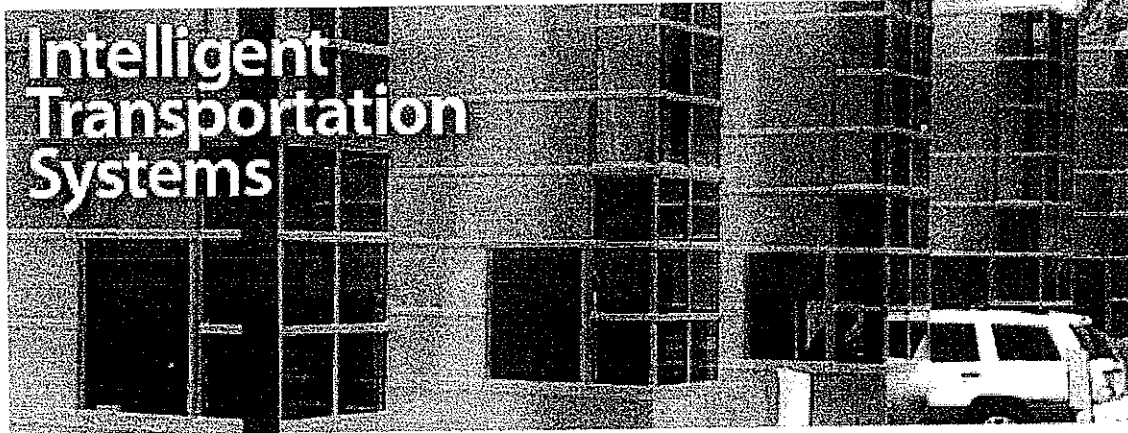
Instructions for License Plate Recognition Vehicles.

1. Turn on Vehicle.
2. Turn on MDC.
3. Open the PAGIS Application on the MDC.
4. At the logon screen enter LAPD in both the username and password field.
5. In the Location field enter your 3-digit Division Code followed by a - and then your shop number. (ie. SOW-89123, HWD-89222)
6. Press the LOGON button.
7. Press the Begin Shift button between 2-3 times. You will see the screen switch and it will begin downloading the hotlists. Once this process is completed you will see a screen with two white panels on it. Underneath the white panels will be buttons COL IR and Take Pic
  - 7A. If you do not see the two white panels, and you do a quick drive around the lot and the system does not capture any plates, pull over to a safe spot. In the trunk, slide out the tray. On the back of the Motorola Computer you will see a USB stick with a clear end. The end should be glowing green to indicate the computer is on. If this is not glowing green, press the white power button on the front of the computer. The usb stick will begin flashing and after approx 30 seconds glow solid green. Should the usb stick fail to glow green, There is a problem with the device and it will need to be serviced. Please contact Tactical Technology Section at 213-996-1330 to have the unit serviced.
8. If you do see the white panels, and as you drive, the system is capturing plates then there is nothing left to do in order to use the system. Each plate is compared to hotlists of Stolen and Felony vehicles and you will hear a siren as well as get a visual message on the screen should the system read one of these types of plates. Make sure to verify the status of the vehicle prior to taking enforcement action as vehicles are entered into and taken out of the system all the time, yet the hotlists are only updated by DOJ every 6 hours.
9. At the end of your shift, shutdown MDC as usual and you are done. There are no special end of watch procedures necessary with the LPR system.



[Click Here to Navigate the US or Rest of the World Sites](#)

- [Home](#)
- [About PIPS](#)
- [About ALPR](#)
- [Applications](#)
- [Products](#)
- [News & Info](#)
- [Partners & Links](#)
- [Contact](#)



**In The News**

PIPS Ann...  
02nd Sept

Idaho Get...  
25th Augu

North Stra...  
25th July

Kenner Pc...  
28th June

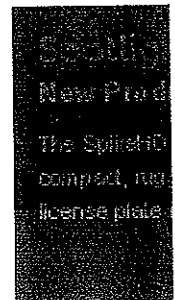
**PIPS Success Stories**

Our ALPR technology helps people and companies every day. Watch our videos now.

[more »](#)

**PIPS Technology – the Most Advanced License Plate Recognition Systems in the World**

PIPS Technology is an industry leader in the development and manufacture of ALPR (Automated License Plate Recognition) systems. Our broad range of ALPR products provide the next generation of information technology for Travel Time Measurement, Law Enforcement, Tolling, Congestion Charging, Access Control, Traffic Monitoring and Automated Site Security Solutions. PIPS products are manufactured to ISO 9001:2000 standards.



[Home](#) | [About PIPS](#) | [About ALPR](#) | [Applications](#) | [Products](#) | [News & Information](#) | [Partners & Links](#) | [Contact](#)  
© 2011 PIPS Technology. A Federal Signal Company. All Rights Reserved.



[Sitemap](#) | [Legal](#) | [Privacy Policy](#)

**ISIDORE GUTIERREZ - Re: Manual for License Plate Recognition Vehicle**

---

**From:** TACTECH TACTECH  
**To:** GUTIERREZ, ISIDORE  
**Date:** 10/4/2011 2:41 PM  
**Subject:** Re: Manual for License Plate Recognition Vehicle

---

Instructions for License Plate Recognition Vehicles.

1. Turn on Vehicle.
2. Turn on MDC.
3. Open the PAGIS Application on the MDC.
4. At the logon screen enter LAPD in both the username and password field.
5. In the Location field enter your 3-digit Division Code followed by a - and then your shop number. (ie. SOW-89123, HWD-89222)
6. Press the LOGON button.
7. Press the Begin Shift button between 2-3 times. You will see the screen switch and it will begin downloading the hotlists. Once this process is completed you will see a screen with two white panels on it. Underneath the white panels will be buttons COL IR and Take Pic
  - 7A. If you do not see the two white panels, and you do a quick drive around the lot and the system does not capture any plates, pull over to a safe spot. In the trunk, slide out the tray. On the back of the Motorola Computer you will see a USB stick with a clear end. The end should be glowing green to indicate the computer is on. If this is not glowing green, press the white power button on the front of the computer. The usb stick will begin flashing and after approx 30 seconds glow solid green. Should the usb stick fail to glow green, There is a problem with the device and it will need to be serviced. Please contact Tactical Technology Section at 213-996-1330 to have the unit serviced.
8. If you do see the white panels, and as you drive, the system is capturing plates then there is nothing left to do in order to use the system. Each plate is compared to hotlists of Stolen and Felony vehicles and you will hear a siren as well as get a visual message on the screen should the system read one of these types of plates. Make sure to verify the status of the vehicle prior to taking enforcement action as vehicles are entered into and taken out of the system all the time, yet the hotlists are only updated by DOJ every 6 hours.
9. At the end of your shift, shutdown MDC as usual and you are done. There are no special end of watch procedures necessary with the LPR system.



**THE LOS ANGELES POLICE DEPARTMENT, MAJOR CRIMES  
DIVISION STANDARDS AND PROCEDURES APPROVED BY THE  
LOS ANGELES BOARD OF POLICE COMMISSIONERS ON:**

**PREAMBLE**

The Board of Police Commissioners (Board) recognizes terrorist activity as the existence in society of individuals and groups who plan, threaten, finance, aid/abet, attempt or perform unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.

The right of public expression through demonstration is expressly recognized and shall not, absent the reasonable suspicion to believe that there may be a potential for a "significant disruption of the public order," as defined in these Standards and Procedures, be subject to Major Crimes Division investigation that involves the maintenance of intelligence files.

Recognizing that terrorist-related intelligence information, properly gathered, analyzed, stored, maintained and disseminated, is essential to the performance of the Department's mandated duty to protect the public through crime prevention, the Board establishes these Standards and Procedures to provide for the legitimate needs of law enforcement while, at the same time, steadfastly respecting all constitutional and statutory rights guaranteed to every individual.

Generally, the focus of an intelligence investigation is strategy oriented. It focuses on the goals or potential of an individual, group or enterprise rather than on specific violations of law. The objective is not arrest and prosecution of suspects but rather the detection, collection, analysis and dissemination of information for the purpose of developing a strategy for crime prevention. Criminal investigations are case-oriented and focus on specific violators of law and specific violations for the purpose of arrest and prosecution after a crime has been committed.

These Standards and Procedures pertain only to Major Crimes Division's Intelligence function. They do not pertain to any Department function that is primarily responsible for conducting criminal investigations and does not maintain "Intelligence Files" as defined in these Standards and Procedures.

## PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

### I. DEFINITION OF TERMS

**Agent Provocateur:** An individual employed, directed, encouraged or allowed to associate with target members or groups in order to incite them to illegal action.

**Attempt:** An act done with intent to commit a crime and tending to, but falling short of, its commission.

**Dissemination:** The communication of any Major Crimes Division Intelligence File information to any person not assigned to Major Crimes Division's direct chain of command. All disseminations must be based upon a right to know and need to know.

**File:** A collection of information including, but not limited to, reports, photographs, documents, printed materials, tape recordings, videotape, computer information or other writings that are kept separately from Intelligence Files. A File may include Initial Lead, Preliminary Investigation, Intelligence Control Center, or Terrorist Threat Assessment Center information.

**Informant:** Generally, an informant is a person who provides information on a recurring basis and/or in exchange for consideration regarding specific criminal activity and who acts under the direction of an investigator.

**Initial Lead Investigation:** The lowest level of intelligence investigative activity which allows a limited follow-up of initial lead information, generally received from the public but may include Department and other law enforcement sources; of such a nature that some follow-up as to the possibility of terrorist activity is warranted. The Initial Lead Investigation threshold need not rise to the reasonable suspicion standard of a Preliminary Investigation and shall be concluded within a 60-day period. Initial lead information shall be stored separately from intelligence files. Only information that meets the reasonable suspicion standard, based on reliable information, may be placed in intelligence files.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

**Intelligence Control Center:** A temporary function performed by Department personnel to gather and coordinate intelligence information during the course of a potential or actual unusual occurrence.

**Intelligence File:** An Intelligence File contains the investigative intelligence information gathered, received, developed, analyzed and maintained pursuant to an open Intelligence Investigation, for the purpose of identifying terrorist individuals, terrorists groups, and victims of terrorism.

**Investigator's Working Folder:** The Working Folder is retained by the assigned investigator and is specifically designated to contain the investigative materials gathered, received, and developed for the specific purpose of updating an approved ongoing Open Intelligence Investigation. However, the Working Folder shall not be part of the Open Intelligence File.

**LAPD Sensitive Work Environment (SWE)/Sensitive Compartmented Information Facility (SCIF):** A facility requiring a national security clearance for access, housed within the LAPD Police Administration Building, in which classified FBI Joint Terrorism Task Force (JTTF) directed intelligence investigations are processed and handled by JTTF members, assigned to CT 10.

**Maintenance:** The process of recording, collating, analyzing, evaluating, indexing, updating, securing, retaining, and purging Intelligence File information gathered pursuant to a Major Crimes Division Open Intelligence Investigation.

**Monitoring:** The short-term or preliminary act of observing or watching the activities of an individual or organization by Major Crimes Division Intelligence investigators for the purposes of gathering information relevant to an Initial Lead Investigation, Preliminary Intelligence Investigation or Open Intelligence Investigation. This short-term monitoring activity shall not rise to the level of "Surveillance" as defined in these Standards and Procedures.

**Need to Know:** A precondition for the communication of intelligence information to entities outside Major Crimes Division or its immediate chain of command.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

**Open Investigation:** An intelligence investigation which has met the reasonable suspicion standard, is based on reliable information and has been approved by the Commanding Officer, Major Crimes Division.

**Organizations:** Any association or group of individuals.

**Pending Activity:** A future event possibly requiring operational planning for policing or police services.

**Plan:** Organized activity by individuals in preparation for the accomplishment of an illegal action involving possible terrorist activity.

**Preliminary Investigation:** A limited intelligence investigation approved by the Commanding Officer, Major Crimes Division, to develop existing information to the point of reliability in order to establish reasonable suspicion based on reliable information.

**Reasonable Suspicion:** An honest belief, based on known articulable circumstances, which would cause a reasonable and trained law enforcement officer to believe that some activity, relating to a definable criminal activity or enterprise, may be occurring or has a potential to occur. (This term is in accordance with Department of Justice definition: 28 CFR Part 23).

**Reliable Information:** Information that is trustworthy or worthy of confidence.

**Right to Know:** The authority or privilege to receive Major Crimes Division Intelligence information.

**Significant Disruption of the Public Order:** Pertains only to public demonstrations involving unlawful acts which can reasonably be expected to result in death, serious bodily injury or property damage and which are intended to have such results to further societal objectives, to influence societal action or to harass on the basis of race, religion, national origin, or sexual orientation. The mere fact of a potentially large demonstration shall not, by itself, constitute a significant disruption of the public order.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

**Storage/Storing:** To provide a place in which any file is kept for the purpose of records retention and not for the purpose of updating. All stored information is kept separate from Open Intelligence Files.

**Surveillance:** The continuous or prolonged observation of a targeted individual or group by clandestine means for the purpose of collecting information material to an approved Preliminary Intelligence Investigation or Open Intelligence Investigation.

**Target:** The subject of an approved investigation.

**Terrorist Activity:** Individual(s) or group(s) who plan, threaten, finance, aid/abet, attempt or perform unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.

**Note:** Activity as it relates to individuals involved in public demonstrations must rise to the level of "Significant Disruption of the Public Order" standard, as defined in these Standards and Procedures.

**Terrorist Threat Assessment Center:** A permanent entity of the Department, staffed by Major Crimes Division personnel to receive, analyze, investigate and communicate terrorist related information.

**Threaten:** The advocacy of, or a statement of intention to commit a criminal act where such advocacy appears to be a viable threat.

**Undercover Investigation:** An approved intelligence investigation involving the use of an undercover officer who clandestinely obtains information about individuals or organizations through the development of ongoing relationships with such individuals or organizations

**Undercover Officer:** A Los Angeles Police Officer who, pursuant to an approved terrorist investigation, clandestinely obtains information about individuals or organizations through the development of ongoing relationships with such individuals or organizations.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**Unusual Occurrence (UO):** An event involving potential or actual personal injury and/or property damage arising from fire, flood, storm, earthquake, tidal wave, landslide, wreck, enemy action, civil disturbance, or other natural or man-caused incident necessitating the declaration of a Tactical Alert or Mobilization. (*Emergency Operations Policies & Procedures - Volume 1 of the LAPD Emergency Operations Guide 11*)

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**II. STATEMENT OF PRINCIPLE**

- A. These Standards and Procedures govern the collection, maintenance, storage and dissemination of intelligence information by the Major Crimes Division intelligence function. These Guidelines also govern the collection, maintenance and dissemination of intelligence information by all other functions and personnel of LAPD when their primary responsibility is gathering intelligence information.

In establishing these Guidelines, the Board of Police Commissioners provides for the legitimate needs of law enforcement within limits created by constitutional and statutory protections which guarantee rights: (1) of privacy, (2) to receive, hold and express ideas, (3) to dissent freely, (4) to write and to publish, (5) to petition for the redress of grievances, (6) and to associate publicly and privately for any lawful purpose.

- B. In reaching the delicate balance of protecting the rights of individuals and providing for effective prevention of terrorist activity, community peace, and in recognizing that no other aspect of the Department's duties requires such detached and sensitive judgments on the part of individual peace officers and that nowhere else is reverence for the law more demanded, the Board affirms the following principles:
1. The Department has a policy of absolute prohibition against the use of illegal or unauthorized methods of collecting, maintaining or disseminating intelligence information; a policy which shall remain in full force and effect. The Commanding Officer, Major Crimes Division, shall report to the Chief of Police any intelligence activity reasonably believed to be contrary to the scrupulous observation of this principle.
  2. The Department considers it both unnecessary and wrong to maintain an intelligence file on any individual or organization unless the reasonable suspicion standard for an Open Intelligence Investigation according to these Standards and Procedures has been met.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

3. Major Crimes Division Intelligence Section personnel shall not collect, maintain or disseminate information about an individual's sexual, political or religious activities, beliefs or opinions unless such information is material to an approved investigation.
4. Major Crimes Division Intelligence Section personnel shall exercise due caution and discretion in the use of information, collected, maintained and disseminated so as not to interfere with the lawfully exercised rights of any person.

### **III. FUNCTIONS AND OBJECTIVES**

- A. The primary objective of Major Crimes Division's Intelligence Operation is the prevention of terrorist activity in the City of Los Angeles and environs by:
  1. Identifying terrorist trends.
  2. Examining terrorist tactics, developing terrorist profiles, assessing terrorist threats, and developing information to protect potential targets.
  3. Investigating, identifying and monitoring individuals and groups that may be engaged in terrorist activity.
  4. Maintaining intelligence files on individuals and groups that may be engaged in terrorist activity.
  5. Assessing and analyzing the capabilities of terrorist individuals or groups, and providing concerned Department entities with sufficient information to thwart their terrorist goals.
  6. Assisting other subdivisions of the Department and other law enforcement agencies to prevent terrorist activities.
- B. A secondary objective of Major Crimes Division Intelligence Section is to advise the Chief of Police and other executive management personnel about pending events which may require operational awareness or planning for policing or police services.



**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

- C. The focus of Major Crimes Division activity is on the safety of persons and protection of property through the prevention of terrorism in the City of Los Angeles. The Board is aware, however, that terrorists do not respect municipal boundaries. It is therefore appropriate to gather intelligence on international terrorists and other persons and organizations whose conduct can reasonably be expected to affect the City of Los Angeles. Similarly, information may be gathered with respect to persons residing in Los Angeles who may commit acts of violence elsewhere and then return. In fulfilling these responsibilities, Major Crimes Division may work with other agencies and pursue investigations into other jurisdictions.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

### **IV. INTELLIGENCE INVESTIGATIVE ACTIVITY**

Generally, the focus of an intelligence investigation, (usually of a long-term nature), is the group or individual enterprise, rather than just individual participants and specific unlawful acts. The immediate purpose of such an investigation is to obtain information concerning the nature and structure of a group or enterprise, including information relating to the group's membership, finances, geographical dimensions, past and future activities, and goals. This is done with a view toward detecting and preventing unlawful acts which are intended to have such results to further their societal objectives, to influence societal action or to harass on the basis of race, religion, national origin, or sexual orientation.

The objective of the Major Crimes Division intelligence investigation is not the arrest and prosecution of suspects, but rather the detection, collection, analysis and dissemination of information for the purpose of crime prevention.

#### **A. LEVELS OF INTELLIGENCE INVESTIGATIVE ACTIVITY**

The Standards and Procedures for Major Crimes Division provide for a graduated level of investigative activity and allow Major Crimes Division the necessary flexibility to act well in advance of the commission of a planned terrorist attack. The three levels of investigative activity are: (1) Initial Lead Investigations, (2) Preliminary Investigations, and (3) Open Investigations.

Whether it is appropriate to open an investigation immediately, or first to engage in a limited follow-up of lead information, depends on the circumstances presented. If the available information shows at the outset that the threshold standard for a Preliminary or Open Investigation is satisfied, then approval to conduct the appropriate investigative activity may be requested immediately, without progressing through the more limited investigative stage. However, if the reasonable suspicion standard has not been met, only an Initial Lead Investigation may go forward.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

Major Crimes Division personnel shall operate the Terrorist Threat Assessment Center which is responsible for the follow-up of Initial Lead Investigations involving possible terrorist-related information.

### **INITIAL LEAD INVESTIGATIONS**

The lowest level of investigative activity is the prompt and limited follow-up of initial leads, many of which are initiated by the public. Checking of leads should be undertaken whenever information is received of such a nature that some follow-up as to the possibility of terrorist activity is warranted. This limited activity should be conducted with an emphasis toward promptly determining whether further investigation, either a Preliminary Investigation or an Open Investigation, should be conducted.

Many initial investigative leads from the public and other sources are expected to be somewhat vague and may not meet the reasonable suspicion standard for a Preliminary or Open Investigation. However, public safety demands a limited but prompt follow-up investigation. The authority to conduct inquiries, short of a Preliminary or Open Investigation, allows Major Crimes Division to respond in a measured way to ambiguous or incomplete information.

### **INVESTIGATIVE TECHNIQUES FOR INITIAL LEAD INVESTIGATIONS**

The following investigative techniques are authorized for Initial Lead Investigations:

- (a) Examination of records available to the public (open source);
- (b) Examination of LAPD records;
- (c) Examination of available federal, state, local government records, etc;
- (d) Interview of the person reporting;
- (e) Interview of the potential subject;
- (f) Interview of witnesses;
- (g) Monitoring.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

Initial Lead Investigations shall be completed within 60 days from the date of receipt of the specific lead. All materials collected during the Initial Lead Investigation shall be stored separately from Intelligence Files unless the initial investigation results in an approved Open Investigation.

### **PRELIMINARY INVESTIGATIONS**

The next level of investigative activity, a Preliminary Investigation, should be undertaken when there is information or an allegation which indicates the possibility of terrorist activity. Preliminary Investigations are based on reasonable suspicion only and are for the purpose of determining whether or not the information or allegation can be developed to the point of reliability.

A Preliminary Investigation may be initiated when:

- Reasonable suspicion exists that an individual or organization may be planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts;
- The results of which are intended to further their societal objectives, influence societal action or harass on the basis of race, religion, national origin, or sexual orientation.

A Preliminary Investigation shall commence when the Commanding Officer, MCD, approves the request. The Preliminary Investigation shall not exceed 120 days.

### **INVESTIGATIVE TECHNIQUES FOR PRELIMINARY INVESTIGATIONS**

A Preliminary Investigation shall not involve the use of electronic surveillance that requires a court order. All other approved investigative methods are authorized.

### **OPEN INVESTIGATIONS**

The commencement of each Open Investigation shall be approved by the Commanding Officer, MCD, who shall ensure the reasons for initiating the investigation meet the required threshold as stated below.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

An Open Investigation may be initiated when there exists, a reasonable and articulated suspicion based upon reliable information that an individual or organization may be:

- Planning, threatening, attempting, performing, aiding/ abetting, or financing unlawful acts;
- The results of which are intended to further their societal objectives, influence societal action or harass on the basis of race, religion, national origin, or sexual orientation.

### **INVESTIGATIVE TECHNIQUES FOR OPEN INVESTIGATIONS**

All lawful investigative technique may be used in an Open Investigation.

#### **B. PENDING ACTIVITY REPORTS**

1. Major Crimes Division Intelligence Section personnel may collect and disseminate information regarding events significant to the City of Los Angeles. Such events include, but are not limited to: parades, demonstrations, dignitary visitations, and VIP appearances, which require operational awareness or planning for policing or police services.
2. Pending Activity Reports are subject to the constraints delineated in the Preamble to these Standards and Procedures and shall be stored separately from Major Crimes Division's Intelligence Files.
3. Pending Activity Reports shall be transmitted to the appropriate Department operational entities immediately upon completion and approval. A copy shall be filed at the Department Command Post. Major Crimes Division shall maintain a log of such reports for audit purposes.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**C. INTELLIGENCE CONTROL CENTER FUNCTION**

1. The Intelligence Control Center collects and disseminates intelligence information gathered during an unusual occurrence or a potential unusual occurrence.
2. Major Crimes Division Intelligence Section personnel may be temporarily assigned to the Intelligence Control Center.
3. While completing the work of the Intelligence Control Center, members of Major Crimes Division are not subject to these Standards and Procedures.
4. All materials gathered, organized and produced during an Intelligence Control Center activation shall be stored separately from Major Crimes Division's intelligence files. Information obtained during an Intelligence Control Center Activation that may be material to an intelligence investigation may only be accessed with approval of the Commanding Officer, Major Crimes Division.

**D. TERRORIST THREAT ASSESSMENT CENTER FUNCTION**

1. The Department has established the Terrorist Threat Assessment Center as the permanent clearinghouse for terrorist-related information specific to the City of Los Angeles or that may impact the City of Los Angeles.
2. The Terrorist Threat Assessment Center shall be responsible for receiving, analyzing, disseminating and conducting a limited intelligence investigation of terrorist-related threats and information.
3. In order to facilitate the dissemination of terrorist-related threats, the Terrorist Threat Assessment Center shall maintain special liaison with appropriate Department and City functions, as well as the Los Angeles County Terrorism Early Warning Group, the California Anti Terrorism Information Center,

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

The United States Department of Homeland Security and the Federal Bureau of Investigation.

4. The Terrorist Threat Assessment Center shall be staffed by Major Crimes Division Intelligence Section personnel. While completing the work of the Terrorist Threat Assessment Center, Major Crimes Division Intelligence Section personnel are subject to these Standards and Procedures. All materials gathered, organized and produced during a Terrorist Threat Assessment Center investigation shall be stored separately from Major Crimes Division Intelligence Files unless the Initial Lead Investigation develops into an approved Open Intelligence Investigation.

**E. MULTI-AGENCY TASK FORCE**

Members of Major Crimes Division, with the approval of the Chief of Police, may be assigned to a multi-agency task force. Major Crimes Division personnel that are members of a multi-agency task force, headed by another agency, may engage in the investigative methods legally authorized for use by that agency, as long as those methods do not violate current laws.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**V. LIMITATIONS AND PROHIBITIONS**

Major Crimes Division Intelligence Section personnel shall recognize and abide by legal and policy limitations placed upon their investigations. In addition to the parameters established by these Standards and Procedures, the following specific limitations and prohibitions apply to Major Crimes Division Intelligence Section personnel and investigations:

- A. No member of Major Crimes Division may engage in any unlawful activity in the collection, maintenance or dissemination of intelligence data or information.
- B. No member of Major Crimes Division may knowingly employ or direct any individual to illegally engage in the collection, maintenance or dissemination of intelligence data or information.
- C. No member of Major Crimes Division may act or knowingly engage another individual to act as an agent provocateur.
- D. No member of Major Crimes Division may employ the use of restricted electronic surveillance equipment without conforming to policy as stated in the Department Manual.
- E. Initial Lead Investigations shall not exceed 60 days.
- F. A Preliminary Investigation shall not exceed 120 days.



## **VI. UNDERCOVER INVESTIGATIONS, SURVEILLANCE AND INFORMANTS**

The Board of Police Commissioners recognizes its critical task in balancing the needs of law enforcement in its efforts to protect the broader society, versus the need to safeguard individual rights guaranteed by a democratic people. Necessarily involved in this process is the recognition that a few groups and individuals espouse, finance, aid or abet violence and/or the wanton destruction of property and that many such groups have attained a high level of criminal sophistication. It is that same criminal sophistication that causes law enforcement to resort to the use of undercover operations, surveillance and informants to counteract their progress. However, as serious as these concerns are, they do not outweigh the previously mentioned societal rights. It is imperative that constitutionally guaranteed rights remain the focal point when utilizing these investigative methods. The law enforcement intelligence community must therefore make optimum use of appropriate resources when available and maximize its capabilities while operating within legal and ethical constraints.

### **A. UNDERCOVER INVESTIGATIONS – SAFEGUARDS**

An investigation involving the infiltration of an organization or the development of an ongoing relationship with an individual by an undercover officer is the most reliable tool for information gathering by law enforcement. The value of the information so obtained has been repeatedly demonstrated in the prevention of terrorist activity and other criminal acts.

The use of information gained in undercover operations is greatly diminished if the manner in which it is obtained casts aspersions upon the conduct of the undercover officer. The conduct of the officer and control of the investigation is therefore critical to minimize interference with lawfully exercised rights. The Chief of Police and the Board of Police Commissioners are charged with great responsibility in authorizing undercover investigations, and should do so only after all other reasonable investigative methods have been determined to be impractical or ineffective to accomplish the objectives of the investigation.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

It is most important that the selection, training, and oversight of undercover personnel receive the utmost attention. It is also imperative that undercover officers understand constitutional and statutory rights which govern their intelligence gathering limits.

The Chief of Police shall have the authority and responsibility to use all resources available to protect the identity and safety of an undercover officer and to protect the confidentiality of information obtained in an undercover investigation.

These Standards and Procedures establish the limits and guidelines by which the conduct of Major Crimes Division Intelligence Section personnel and undercover investigative techniques are controlled.

### **B. UNDERCOVER INVESTIGATION COMMITTEE**

The President of the Board of Police Commissioners or another Commissioner designated by the President shall comprise the Undercover Investigation Committee. The Commissioner comprising that Committee shall serve a maximum of three consecutive years, and shall have the duties and assignments as prescribed by these Guidelines.

### **C. UNDERCOVER INVESTIGATION – AUTHORIZATION**

1. Undercover investigations (i.e. use of an undercover officer) may be initiated subject to the following safeguards:

- a. The targeted individual(s) and/or organization have been approved for a Preliminary or Open Investigation.
- b. No undercover investigation shall be commenced without the written approval of the Chief of Police and the Committee. Prior to the actual commencement of any infiltration by an undercover officer, the requirements set forth below must be met:

**Exception:** In an emergency involving a life threatening situation where the Undercover Committee is unavailable, an undercover investigation may be commenced with the approval of

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

the Chief of Police. Telephonic notification to the Undercover Committee shall be made as soon as possible and written approval from the Undercover Committee shall be requested within 72 hours.

- 1) The undercover investigation application shall be signed by the Commanding Officer, Major Crimes Division, through the chain of command to the Chief of Police;
- 2) All supporting assertions of fact in the application shall be contained in affidavits (or declarations under oath); said affidavits or declarations may be based on hearsay evidence. The requirements for these affidavits shall meet the requirements of these Guidelines (and shall not be equated with the requirements for a search warrant).
- 3) The application shall include information which bears upon:
  - (a) Whether there is a reasonable suspicion to believe that the target individual or organization may be planning, threatening, financing, aiding/abetting, attempting or performing unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation;
  - (b) The expected results of the undercover operation in terms of prevention of terrorist activity;
  - (c) The anticipated manner in which the undercover operation will be conducted, including likely individuals and organizations who will be contacted;
  - (d) The authorized duration of the undercover investigation and the provision for periodic review;
  - (e) What other methods have been previously used and why Major Crimes Division believes that an undercover

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

investigation is the only practical means to accomplish the objectives of the investigation;

- (f) If the Department intends that the undercover officer shall infiltrate a non-target organization, then there shall be included additional information which clearly indicates the need to become a member of the non-target organization. No information on the non-target organization or its members will be reported in any intelligence file, unless there is reasonable suspicion to believe that the non-target organization, or members of the non-target organization, may be involved in terrorist activity or in cases of public demonstration, activities which may have the potential to significantly disrupt the public order.

- c. The Committee shall not issue written authorization initiating an undercover investigation of an individual or organization unless the Committee agrees that all of the following requirements have been met:

- 1) The application has been signed by the officials listed in subparagraph C.1.b(1) above;
- 2) All supporting assertions of fact are sworn to under oath; and
- 3) The Committee has consulted with legal counsel for advice, as necessary.

The Committee shall maintain a written record of compliance with this subparagraph.

- 4) The Committee renders written findings that:
  - a. There is an approved Preliminary or Open Intelligence Investigation which meets the respective reasonable suspicion standard;

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

- b. That other means are unavailable or ineffective to achieve the investigative objectives of the Department; and
  - c. That the interests of privacy and free expression are outweighed by the nature and magnitude of the likely harm.
- 5) Where the Department seeks to infiltrate a non-target organization so that an undercover officer may infiltrate the target organization, the Committee shall render additional written findings that:
- a. All other means of obtaining sufficient information on the target organization either have been tried without success or are not practical; and
  - b. There is reasonable basis for believing that the presence of the undercover officer in the non-target organization will enable him/her to infiltrate the target organization as evidenced by the fact that:
    - i. That the target organization recruits members from the active members of the non-target organization;
    - ii. That membership in the non-target organization is a condition of membership in the target organization; or
    - iii. There is a substantial link between the non-target organization and target organization, equal to those described in (i)-(iii) above, which otherwise justifies the undercover officer's infiltration of the non-target organization; provided, however, that this substantial link shall not be based solely on the evidence that:
      - I. The non-target organization espouses or holds the same political, social or economic

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

positions as the target organization (e.g. a non-violent organization which opposes nuclear power plants shall not be infiltrated in order to infiltrate a target organization which opposes nuclear plants by violent means unless there are other factors present);

II. The non-target organization shares the same racial, religious or other status or concerns with the target organization.

d. The interests in privacy and free expression of the non-target organization are outweighed by the nature and magnitude of the likely harm by the target organization. In this regard, the Committee shall consider, in part, former and other current infiltrations by undercover officers of the non-target organization.

e. Where the Committee finds that the application for an undercover investigation meets the requirements set forth in paragraph c.1-5 (Pages 16-17), it shall issue written authorization to conduct an undercover investigation under the following terms and conditions:

- 1) Specifying the individual or organization that is the target of the undercover investigation;
- 2) Setting forth limitations, if any, on the activities which can be engaged in by the undercover investigators with regard to the target individual or organization;
- 3) Imposing a time limit on the undercover investigation, which, however, cannot exceed a period of one year with a semi-annual status review by the Undercover Committee;
- 4) If the infiltration of a non-target organization also has been approved, the written confirmation shall include these additional terms and conditions:

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

- a) Specify the number of meetings of the non-target organization, which the undercover officer may attend without further approval of the Committee;
  - b) Set forth limitations, if any, on the activities which can be engaged in by the undercover officer in the non-target organization;
  - c) Require quarterly reports from Major Crimes Division regarding the steps taken by the undercover officer to infiltrate the target organization, estimates of the additional time necessary to infiltrate the target organization and an explanation of the reason why the target has not yet been infiltrated;
  - d) Require quarterly reviews by the Committee on whether the infiltration of the non-target organization still meets the requirements set forth in paragraph c.1-5 (Pages 16-17), above.
- f. The Committee shall make its decision within 72 hours of receipt of the application of the Department. In the event that the Committee is unable to render a decision within this time frame, the Chief of Police may present the matter to the full Board for a determination. The Board's determination shall be made in accordance with the Undercover Standards and Responsibilities Section of these Standards and Procedures.
- g. If the Department seeks to continue an undercover investigation after the initial one-year period, the Department shall request that the investigation be reviewed by the Committee.
- 1) The request for review shall include all information previously submitted and, in addition, shall contain information on all activities of the undercover officer during the preceding investigation, including all

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

organizations and individuals which were contacted by him/her in that time period.

- 2) The Committee shall issue written authorization to continue an undercover investigation of a target organization or individual only where in the preceding one-year period:
  - a) The undercover officer has obtained some reliable information that the target may still be a viable threat in terms of planning, threatening, financing, aiding/abetting, attempting or performing unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.
  - b) The undercover officer has taken all reasonable steps to develop the necessary contacts with the target organization or individual so as to ascertain whether said target is conducting activities described in paragraph 2.a. above, but the undercover officer has been unable to develop such contacts through no fault of his/her own.
- h. Except as permitted in paragraph VI.C, no undercover investigation shall be conducted absent compliance with the above-mentioned procedures.
- i. Unless already approved under VI.C.L.c(4) above, during a duly authorized undercover investigation, an undercover officer may be present on two occasions in organizations which are not the subject of a Major Crimes Division Intelligence investigation. Once the undercover officer has attended two such meetings, functions, demonstrations or other activities (whether public or private), the attendance of the undercover officer at these



**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

activities shall be reported in writing to the Commanding Officer, Major Crimes Division, the Chief of Police and the Committee. The undercover officer shall not attend any further meetings, functions, demonstrations or other activities of the non-target organization except under either of the following circumstances:

- 1) The failure of the undercover officer to attend such activities will expose him/her to immediate danger to his/her physical safety or jeopardize the fictitious identity of the undercover officer. In this event, the undercover officer's attendance at these additional activities of the non-target organization shall be reported in writing to the Commanding Officer, Major Crimes Division, the Chief of Police and the Committee.
- 2) The Committee gives written authorization for the undercover officer to attend further activities of the non-target organization for the purpose of maintaining a cover, but only in accordance with the guidelines and findings set forth in Section VI.C.1c(4).
- 3) The events and writings pertaining to (1) and (2) above shall be audited by the Commission pursuant to Section IX, infra, to ensure compliance with these Guidelines.

**D. REVIEW BY THE BOARD OF POLICE COMMISSIONERS**

1. Each member of the Board of Police Commissioners shall have the right to request a review by the entire Board of any decision by the Committee and to have access to such information as may be necessary to make a determination as to whether such a request is appropriate. In addition, in the event that the Committee does not confirm the infiltration by the undercover officer, the Chief of Police may request in writing that the proposed undercover investigation be reviewed by the entire Board. The Board in making its review shall:

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

- a. Consider each and all of the findings made by the Committee (including such other information as the Board may seek from the Committee);
- b. Prepare written findings if the Board rejects the decision of the committee. The written findings shall expressly recite the basis for, and facts upon which, the decision to override the Committee was made;
- c. Not override the Committee unless at least three votes in favor of said override are obtained; and
- d. Report to the public on an annual basis the number of decisions reviewed and the number of times the decision of the Committee was changed.

### **E. UNDERCOVER STANDARDS AND RESPONSIBILITIES**

#### **1. UNDERCOVER OFFICER STANDARDS**

- a. **PRESENCE AT RELIGIOUS EVENTS:** Undercover officers shall take all reasonable steps to minimize any intrusion of religious ceremonies, meetings or discussions. Undercover officers shall not report on those events unless they relate to the undercover investigation.
- b. **PARTICIPATION IN PRIVILEGED INFORMATION EVENT:** Undercover officers shall, when possible, avoid attendance at a meeting which would involve information covered by California Evidence Code Sections 954 (Lawyer-Client Privilege), 980 (Privilege for Confidential Marital Communications), 992 (Confidential Communication Between Patient and Physician), 1012 (Confidential Communication Between Patient and Psychotherapist), and 1033 (Privilege of Penitent). If an undercover officer attends a meeting where privileged information is shared, the undercover officer shall not report or divulge the content of said meeting.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**NOTE:** Undercover officers are exempt from this restriction if the holder of the privilege waives same as defined under California Evidence Code Sections 912, 956, 981, 997 and 1018.

- c. **PRESENCE AT EDUCATIONAL INSTITUTION:** If attendance by an undercover officer in an educational institution is required as part of the investigation, the officer shall not report on any activity associated with the institution which is not directly related to the investigation. The undercover officer shall take all reasonable steps to minimize any intrusion which his/her conduct might have in connection with the academic freedoms associated with the institution.
- d. **WRITTEN REPORTS:** Undercover officers shall not make written reports of their operations and activities.
- e. **TRAINING OF UNDERCOVER OFFICERS:** The Officer-in-Charge, Special Assignment Unit, shall ensure each undercover officer is familiar with these sections and is trained regarding acceptable standards of conduct.

**2. UNDERCOVER RESPONSIBILITY**

- a. **OFFICER'S RESPONSIBILITY:** An undercover officer who attends a meeting as described in VI.E.1.a and VI.E.1.b shall report attendance to an investigative or Special Assignment Unit supervisor.
- b. **SUPERVISOR'S RESPONSIBILITY:** An investigative or Special Assignment Unit Supervisor who becomes aware that an undercover officer has attended a meeting as described in VI.E.1.a. shall report such attendance to the Commanding Officer, Major Crimes Division.
- c. **COMMANDING OFFICER'S RESPONSIBILITY:** The Commanding Officer, Major Crimes Division, when notified that an undercover officer has attended two meetings, functions, demonstrations or other activities of any organization not

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

approved for infiltration, shall report such activity to Major Crimes Division's immediate chain of command.

**NOTE:** In connection with religious ceremonies, no reporting beyond the Commanding Officer, Major Crimes Division, is required if the religious nature of the group was considered at the time the undercover operation was approved. The undercover officer shall be directed not to attend any further such meetings, functions, demonstrations or activities of any organization not approved for infiltration unless:

Failure of the undercover officer to attend such activities will pose an immediate danger to the physical safety of the officer or jeopardize his/her identity. In this event, the undercover officer's attendance at these additional activities shall be reported to the Commanding Officer, Major Crimes Division, and Major Crimes Division's immediate chain of command who shall authorize attendance at further activities for the purpose of maintaining cover.

### **3. APPROVAL OF THE BOARD**

Any request to modify current restrictions on acceptable conduct by undercover officers as cited in the Major Crimes Division confidential Procedural Manual shall be considered during an Executive Session of the Board in compliance with the Ralph M. Brown Act.

### **F. SURVEILLANCE AND INFORMANT OPERATIONS**

Surveillance and informant operations are discussed in Major Crimes Division's confidential Procedural Manual. Inclusion of those operations in these Guidelines would have a detrimental effect on operational effectiveness and could jeopardize the safety of officers and informants.

## **VII. CONTROL OF INTELLIGENCE FILES**

- A. The Commanding Officer, Major Crimes Division, shall be responsible for the establishment of written procedures to ensure the security of intelligence files. These procedures shall be made available to the Commission's Audit Committee or designee at any time to monitor compliance with these Guidelines.
- B. The Commanding Officer, Major Crimes Division, shall review all intelligence reports and pending activity reports, prior to their storage.
- C. Information collected by Major Crimes Division Intelligence Section personnel shall not be maintained unless it is material to an investigation authorized under these Standards and Procedures. However, recognizing a determination of materiality is not always possible when information is originally received, an investigator may record information until such time as a determination can be made. Such information shall not become part of the files maintained by Major Crimes Division, and shall be destroyed in accordance with record keeping procedures when it is determined that the information is not material. Initial inquiries and contacts, the working investigation notes, drafts or other writings shall be maintained in the investigator's working folder.
- D. No member of Major Crimes Division Intelligence Section may disseminate information from Major Crimes Division files to any individual or agency that does not have both a need and a right to the information.
- E. No member of Major Crimes Division Intelligence Section may provide a copy of an intelligence report to anyone outside of Major Crimes Division Intelligence Section and Major Crimes Division's immediate chain of command without the prior approval of the Commanding Officer, Major Crimes Division, or the Major Crimes Division Custodian of Records.
- F. Any member of Major Crimes Division Intelligence Section who copies, permits inspection of, or disseminates intelligence information from intelligence files shall record the date, name of officer disseminating, name of the individual receiving, the reason for the dissemination, the information disseminated, and its reliability.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

- G. In the case of a joint investigation by Major Crimes Division Intelligence Section and another law enforcement agency, the Commanding Officer, Major Crimes Division, may authorize a free flow of information on the particular individual(s) and organization(s) being investigated, consistent with the Standards and Procedures of Major Crimes Division.
  
- H. Members of Major Crimes Division Intelligence Section shall not maintain or utilize the Division's intelligence materials outside of their official work location without the written approval of the Commanding Officer, Major Crimes Division.
  
- I. Any writing prepared to summarize the status or activities of an investigation other than that placed on LAPD Form 1.89 (Intelligence Report), shall be recorded on a LAPD Form 15.7 (Employee's Report). The Employee's Report shall be retained and filed by the Commanding Officer, Major Crimes Division, for a period of one-year, after which time it shall be purged at the discretion of the Commanding Officer.

**VIII. PERSONNEL ADMINISTRATION**

- A. Recognizing the importance and sensitivity of the duties performed by Major Crimes Division, the Department will exercise special care and attention to the selection, development, training, and retention of all personnel assigned to Major Crimes Division.
- B. These Standards and Procedures shall be distributed to, and made the subject of training for, all Major Crimes Division Intelligence Section personnel.
- C. All Major Crimes Division Intelligence personnel shall be required to acknowledge, in writing, their receipt of a copy of these Standards and Procedures, and their willingness to abide by the purpose, procedures, and spirit of its content.
- D. As with any other Department guideline or regulation, any willful or negligent violation of or deviation from these Standards and Procedures will be viewed as misconduct and be subject to appropriate disciplinary action.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

### **IX. AUDITING AND OVERSIGHT**

- A. At least annually, the Inspector General (IG), on behalf of the Board of Police Commissioners, shall audit the operations of Major Crimes Division for compliance with these Standards and Procedures. The IG may enlist the assistance of one administrative support staff member who shall be subject to a background examination and possess the requisite auditing and management expertise to ensure compliance with the Standards and Procedures.

The audit shall consist of, but not be limited to, the following:

- a. A review of all Major Crimes Division Intelligence regulations, rules and policies.
  - b. A review of all Major Crimes Division Intelligence investigations conducted in the prior year.
  - c. A review of all materials gathered, received, developed or maintained by Major Crimes Division Intelligence Section for intelligence purposes.
  - d. An oral interview of Major Crimes Division Intelligence Section personnel assigned to task forces wherein another agency is the lead agency and is in possession of all work product, to ensure that Major Crimes Division personnel are in compliance with these Standards and Procedures. This oral interview is to include MCD Intelligence Section personnel assigned to the LAPD SWE/SCIF ( CT-10).
  - e. A written report setting forth the nature of the audit and the findings on compliance with these Standards and Procedures.
- B. The IG or his/her designated administrative auditor(s) may, at any time, conduct surprise audits or inspections as deemed appropriate to monitor compliance with these Standards and Procedures.



**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

- C. Based upon the audit, the administrative auditor(s), under the supervision of the IG, shall prepare a confidential written report for the entire Board.
- D. From the above confidential report, the Police Commission shall prepare annually, a public report of the audit on the preceeding year's activities of Major Crimes Division.
- E. Annually, the Commanding Officer, Major Crimes Division, shall provide written certification that all current Major Crimes Division intelligence investigations have been internally reviewed and that those Major Crimes Division investigations which are no longer viable have been closed.
- F. The written justification for the commencement of an intelligence investigation shall be retained and reviewed by the Commission during the audit described in Section IX.
- G. The Board shall have the right to review the Major Crimes Division confidential Procedural Manual and approve those portions which pertain to prohibitions on undercover officer conduct previously included in these Standards and Procedures. Any changes to those provisions shall receive prior approval of the full Board, upon recommendation of the Intelligence Committee. Discussion of the contents of the confidential Procedural Manual shall be held in Executive Session of the Board, and shall remain confidential.
- H. Oversight and Auditing of Major Crimes Division Intelligence Section personnel assigned to the LAPD SWE/SCIF (CT-10) (see also, Standard Operating Procedures and Physical Security Requirements - SCIF).
  - 1. Upon receipt of the necessary security clearance(s), the Inspector General for the Los Angeles Board of Police Commissioners will be provided access to the LAPD SWE/SCIF for the purpose of oversight directed at LAPD CT-10 personnel.

## **PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES**

2. In accordance with existing Joint Terrorism Task Force (JTTF) protocols, it is understood that certain LAPD investigations will be converted by the FBI into FBI JTTF investigations when the FBI determines that those investigations meet investigative thresholds under the United States Attorney General Guidelines and the FBI's Domestic Investigations and Operations Guide. These investigations and records pertaining thereto will be maintained within the LAPD SWE/SCIF and are subject to FBI and United States Department of Justice (DOJ) internal inspection and/or auditing processes.<sup>1</sup>
3. In order to meet the objectives of ensuring adherence to federal law pertaining to the confidentiality of files under the control of the FBI, while also accomplishing oversight responsibilities vested in the LAPD Inspector General, the LAPD IG will, in conformance with federal laws and regulations (and with the necessary clearance[s]), have access to audits or inspections conducted by the federal government concerning LAPD CT-10 personnel.
4. Additionally, where the LAPD IG determines that an inspection or audit of a particular facet of LAPD CT-10 personnel is necessary, the Special Agent in Charge of the FBI's Counterterrorism Division (CT SAC), will audit or inspect the particular facet and create a written report for the LAPD IG.
5. Should the IG determine that it is necessary to review classified investigative records/information in order to

---

<sup>1</sup> Specifically, primary oversight for compliance with the United States Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) and the FBI's Domestic Investigations and Operations Guide (DIOG) lies with the United States Justice Department's National Security Division and the FBI's Inspection Division, Office of General Counsel, and Office of Integrity and Compliance. Congressional Oversight is conducted by various committees of the United States Congress, but primarily by the Judiciary and Intelligence Committees. The Intelligence Oversight Board (IOB), comprised of members from the President's Intelligence Advisory Board (PIAB), also conducts oversight of the FBI. Among its other responsibilities, the IOB reviews violations of the Constitution, national security law, Executive Orders and Presidential Decision Directives by the FBI and issues reports thereon to the President and the Attorney General.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

carry out the auditing/oversight of LAPD personnel assigned to CT-10, the IG shall coordinate access to such records and investigations with the CT SAC.

6. At the conclusion of the IG's review of any "classified" inspection/audit, the IG shall prepare a confidential declassified report to the Board of Police Commissioners in which the IG shall assess compliance by LAPD CT-10 personnel with applicable laws, rules, and standards and procedures. Any use of information from an FBI JTTF file, in either its original format or derived there from, must comply with federal laws and regulations. The IG may not reveal classified information in an LAPD IG report. If the information is vital to the report, the IG shall seek permission from the FBI to use that information in a declassified form. Only the FBI can determine whether classified information can be declassified. The IG will consult and gain the concurrence of the FBI's CT SAC prior to any dissemination of information derived from the FBI.
7. If the LAPD IG determines that there is a potential violation of federal law or regulation by an FBI or other federal employee, the IG will refer the matter to the FBI JTTF Assistant Special Agent in Charge for appropriate action.

**PUBLIC ACCESS TO INFORMATION  
STANDARDS AND PROCEDURES**

**X. PUBLIC ACCESS TO INFORMATION**

- A. Major Crimes Division Intelligence Section shall provide public access to all documents maintained or collected by Major Crimes Division Intelligence Section in accordance with the provisions of the Freedom of Information Ordinance (FOIO) of the City of Los Angeles, as interpreted in the opinion of the City Attorney, dated July 8, 1983, and in accordance with any state or local laws which may require or permit greater disclosure of information.
- B. In providing disclosure pursuant to requests made under this section, or other applicable laws, Major Crimes Division Intelligence Section shall evaluate each document within the scope of each such request on an individual document by document basis. Major Crimes Division Intelligence Section shall search documents within each category of documents maintained by Major Crimes Division Intelligence Section (and created after the effective date of these Guidelines) and shall, to the extent reasonably possible, maintain documents in a manner which enables their production in response to such requests.
- C. The Department shall apply the test set forth in subsection "o" of the FOIO to any requests and shall consult with the Office of the City Attorney, as necessary.

## **050. RECORDS RETENTION PROGRAMS.**

**050.08 SUPERVISING.** Commanding officers and section officers in charge shall be responsible for supervising the proper maintenance and disposal of division records by the division record unit, in accordance with Division 12 of the Los Angeles Administrative Code and the Department Records Retention Program.

Obsolete records shall be placed in cardboard cartons, under the direction of an officer, and fastened securely with twine. Each carton shall be marked or tagged, "To be Destroyed," and turned over to the supply truck which delivers division supplies.

**Records Retention Representatives.** Commanding officers and section officers in charge shall designate a Records Retention Representative within their command who shall:

- Inventory and appraise all records in their entity;
- Prepare and maintain Records Retention Schedules for records in their entity;
- Prepare amendments to Records Retention Schedules when necessary;
- Cause records to be transferred to storage when appropriate; and,
- Maintain liaison with the Department Records Coordinator regarding records management procedures.

**050.40 POLICE BULLETINS.** Police Bulletins shall be transferred at the end of each month from the monthly file to the yearly file and retained for two years.

**050.48 POLICE SERVICE LOG, FORM 15.27.00.** Police Service Log, Form 15.27.00, shall be stored at the end of the month and retained for two years.

**050.56 TELETYPE BROADCASTS.** Teletype broadcasts not otherwise filed shall be destroyed after five days.

**050.72 DAILY FIELD ACTIVITIES REPORTS.** The Daily Field Activities Report, Form 15.52.00, and the Traffic Daily Field Activities Report, Form 15.52.01, shall be retained for two years.

**050.80 DAILY WORKSHEET, FORM 15.26.00.** Daily Worksheet, Form 15.26.00, shall be retained for two years.

**050.88 DIVISION FILE FOLDER HEADINGS.** The main headings of subject matter to be filed shall be printed in the upper-left corner of the folder. Following are some of the headings to be used: (Additional headings may be used at the discretion of the record unit supervisor):

- Bulletins.
- Teletype Releases.
- Budget Requests.
- Monthly Reports.
- Automotive Equipment.
- Forms.
- Jail.
- Orders.
- Correspondence.
- Vacation Schedule.
- Property.
- Daily Occurrences Reports.

- Felony and High-grade Misdemeanor Records.
- Traffic.
- Watch Reports.
- Miscellaneous.

## CHAPTER 1 RECORDS RETENTION AND DISPOSITION

Section

- 12.1 Definitions.
- 12.2 Responsibilities.
- 12.3 Records Retention Schedule.
- 12.4 Photographic and Electronic Reproduction.
- 12.5 Destruction of Records.
- 12.6 Use of Descriptive Terms.
- 12.7 Applicability of the Chapter.

**Sec. 12.1. Definitions.**

The following definitions shall apply for purposes of this division.

(a) **APPRAISAL (of records).** The act of determining (1) the relative activity in the use of records; (2) value of records with regard to administrative, legal, fiscal, vital or historical interest; (3) adequate and essential periods of retention; and (4) appropriate disposition of records.

(b) **DEPARTMENT.** Includes City Departments, offices and bureaus.

(c) **DISPOSITION.** Involves either the transfer of inactive records to a city records center or the disposal of such records by destruction, sale as waste paper or other lawful act.

(d) **DUPLICATE RECORDS.** Copies or counterparts, which accurately reproduce original records, whether prepared simultaneously by the same impression as the original, or from the same matrix, or by means of photographic reproduction, including enlargements and miniatures, recorded video images on magnetic surfaces, or by mechanical, video or electronic re-recording, or by chemical reproduction, or by other equivalent technique, and which are not treated as or used for functions or purposes regularly served by such original records in the regular course of City business.

(e) **HISTORICAL RECORDS.** Records which depict persons or phenomena which are or have been a part of events or conditions which significantly affect or have affected the City, its functional activities, its heritage, growth and/or development.

(f) **ORIGINAL RECORDS.** Any public record other than a duplicate as defined in Section 12.1(d). Photographically or electronically reproduced records can also be deemed

original records, provided the reproduction is done in accordance with Section 12.4 of this Code.

(g) **PHOTOGRAPHIC AND ELECTRONIC REPRODUCTION.** Includes all forms of photography, micrographics, or processes which record images electronically or optically.

(h) **PHYSICAL INVENTORY.** A complete listing of records by series title, classification or other designation together with sufficient supporting data to enable a proper evaluation for determining retention periods.

(i) **PUBLIC RECORD.** A record which is made or kept by a City department or office pursuant to law or indicating action taken with respect to a particular City matter, but not including notes or preliminary drafts not retained in the regular course of business or a writing prepared or used by a City department or officer as a temporary aid in the preparation of minutes of a meeting of a City body or other record.

(j) **RECORD.** Any form of communication or representation, including letters, words, pictures, sounds, symbols or combinations thereof, recorded or reproduced upon a tangible object by handwriting, typing, printing, photocopying, photography, recording of images on sensitized or magnetic surfaces, or by other means.

(k) **RECORDS MANAGEMENT PROGRAM.** An administrative plan for application of efficient and economical management methods of identification, appraisal, maintenance, protection, preservation, transfer, retention and disposition of City records.

(l) **RECORDS RETENTION SCHEDULE.** An informational timetable or roster of records by category which primarily lists the minimum periods of time which must elapse, as required by the City or pursuant to state law, whichever is longer, before records in each category identified on said document may be destroyed.

(m) **RECORD SERIES.** Groups of related records which are normally used and filed as a unit and which permit evaluation as a unit for retention and disposition purposes. A record series may contain both forms and correspondence.

(n) **VITAL RECORDS.** Records essential for continuation of service, reconstruction or resumption of the essential operational functions of the City or maintenance of public health, safety and order in the event of a local emergency or public disaster.

**SECTION HISTORY**

Based on Charter Sec. 434.

Amended by: In Entirety, Ord. No. 155,822, Eff. 10-24-81; In Entirety, Ord. No. 168,014, Eff. 7-27-92.

**Sec. 12.2. Responsibilities.**

(a) **CITY CLERK.**

(1) The City Clerk shall be responsible for the Records Management Program of the City and for development, administration and coordination of procedures for those duties. The City Clerk shall also provide for and administer a records center or centers for the efficient and



economical storage, maintenance, and servicing of inactive City records. The City Clerk shall provide uniform standards and efficient controls over the identification, appraisal, maintenance, protection, preservation, transfer, retention, and disposition of City records.

(2) The City Clerk shall also:

A. Provide assistance in the preparation of records retention schedules and amendments thereto;

B. Review records retention schedules and amendments, provide guidelines and make recommendations deemed appropriate to insure coordination in the identification, maintenance, protection, transfer, retention and disposition of all City records; and

C. Receive those records which are not currently required to be used in the regular course of City business and which a department may transfer thereto for maintenance, preservation, and disposition.

(3) The City Clerk shall also develop and maintain a City historical records program, including a City Archives, in connection with which the City Clerk shall:

A. Review records retention schedules and available records from all departments, including those public records of public officials transferred during the term of office of any such official or existing at the termination or expiration of such public official's term of office, and all requests for destruction of records, in order to identify historically significant records;

B. Receive, separate and collect, from each department, with concurrence of the department head or officer involved, historical records not in current use, including but not limited to those which are listed on the records retention schedule, provided that such records are not, or will not be, maintained in the normal course of events in another portion of the City Archives as a part of the minutes or other necessary records of the City;

C. Classify, index and store in the City Archives, where applicable, all records when received which are deemed by the department head or the City Clerk to have historical value;

D. Cause historical records to be suitably protected and preserved;

E. Provide a suitable reference area and document retrieval service for departments, officers, and for researchers of historical information; and

F. Periodically examine records of historical value retained in City departments for current use, and, in conjunction and in cooperation with said departments, provide for the availability of such records during normal business hours in the event such are needed for review or research purposes.

(4) The Office of the City Clerk shall become custodian of any historical record transferred to the City Archives under the terms of an approved records retention schedule, subject to the requirements for records custodianship imposed by the charter on other City officers.

Notwithstanding the foregoing or any provision of any records retention schedule to the contrary, any historical records of the Office of the Mayor or of any Councilmember in the custody of the City Clerk or of any Councilmember may be transferred to a public or private academic institution having suitable library facilities, as provided for in an agreement between the City of Los Angeles and such institution. Such agreement shall include the following provisions:

A. Records so transferred shall remain public records in the custody of the Office of the Mayor, or the involved Councilmember, subject to such control by the institution as is permitted by the terms of the agreement.

B. Records shall be catalogued, preserved, maintained and made available for public inspection at that institution, in accordance with the Public Records Act of the State of California and professional archival standards.

C. Records so transferred may at any time be inspected by City officers and employees for compliance with the terms of the agreement.

D. Upon request of the Office of the Mayor, or the involved Councilmember, with concurrence of the City Council, or request by the Council, with concurrence by the Office of the Mayor, or the involved Councilmember, records shall be promptly returned by the institution.

E. Records transferred may not be sold, licensed, transferred, destroyed or loaned to users except as those activities relate to the City of Los Angeles.

Any such agreement, or amendments thereto, shall be approved by the City Council. No records of the Office of the Mayor created prior to July 1, 1973 may be transferred to any such institution.

(5) Any City record determined by the City Clerk to be of possible interest to a recognized community historical organization, but not of historical interest to the City of Los Angeles, may be given to a recognized community historical organization in lieu of the destruction thereof provided the following conditions are met:

A. The City Clerk has consulted with the department or office having custody of such record or the department or office from which such record was received by the City Clerk regarding the release thereof.

B. The City Clerk has made all the determinations required to be made under Section 12.5(a)(1) of this Code.

C. The City Attorney has concurred in the release of the record.

D. The request to donate has been forwarded to the City Council in the same manner as a Request for the Destruction of Records containing a certification from the City Clerk that the record in question is of possible interest to a recognized community historical organization and that all the determinations required under Section 12.5(a)(1) of this Code have been made. The file shall also contain the response of the City Attorney indicating whether or not the City Attorney concurs in this matter.

E. The City Council has approved the request for transfer of such records.

Upon receipt of said records, the designated community historical organization receiving them shall become the owner thereof and all further disposition of the document shall be at the discretion of such community historical organization.

(b) **OFFICERS AND DEPARTMENT HEADS.** Each officer and the head of each City department, shall:

(1) Be responsible for implementing and maintaining within the particular department involved, an efficient and cost effective records management program, and shall preserve and protect records and information collected and retained in the regular course of City business. The records management program of each department shall insure that the collection, maintenance, use, or dissemination of any record of identifiable personal information is carried out for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information. The records management program of each department shall insure also that no record is maintained describing how any individual exercises rights guaranteed by the First Amendment of the United States Constitution, or Article 1, Sections 1 through 4 of the California constitution, unless expressly authorized by statute or by the individual about whom the record is maintained, or unless pertinent to and within the scope of the duties and responsibilities of the department, provided that the department's activities with respect to the collection, maintenance, use and dissemination of such records are conducted in compliance with City guidelines and regulations which are pertinent to those activities and in compliance with all applicable laws;

(2) Cooperate with the City Clerk to assure proper administration and implementation of the City's Records Management Program;

(3) Certify or be responsible for all certifications required of that officer or department head as set forth in this chapter;

(4) Be responsible for identification, transfer, retention and disposition of the records of said department;

(5) Conform to and implement the records requirements and limitations set forth in Section 12.3 and periodically review said schedule for the purpose of determining whether the retention periods should be changed or items added to or deleted from the schedule and amend the schedule to reflect such changes.

(6) Conform to and implement the record reproduction requirements and limitations set forth in Section 12.4 and as elsewhere in this chapter provided, and;

(7) Conform to and implement the destruction of records requirements and limitations as set forth in Section 12.5 and as elsewhere in this chapter provided;

SECTION HISTORY

Added by Ord. No. 155,822, Eff. 10-24-81.

Amended by: Subsec. (b), Subdiv. (1), Ord. No. 158,139\*, Eff. 8-21-83; In Entirety, Ord. No. 168,014, Eff. 7-27-92; Subsec. (a), Subdiv. (4), Ord. No. 168,846, Eff. 7-30-93; Subsec (a), Subdiv. (5), Ord. No.

171,474, Eff. 2-13-97; Subsec. (b), Subdiv. (5), Ord. No. 171,472, Eff. 2-13-97; Subsec. (a), Subdiv. (4), Ord. No. 171,602, Eff. 6-21-97; Subsec. (a)(1), Ord. No. 173,288, Eff. 6-26-00, Oper. 7-1-00.

\* Freedom of Information Ordinance of 1983.

**Sec. 12.3. Records Retention Schedule.**

(a) **PREPARATION.** In the preparation of a records retention schedule and any subsequent proposed amendments thereto, the officer or department head involved shall cause the following to be accomplished:

(1) Prepare a physical inventory and appraisal of all records created and maintained by the department involved in order to determine the relative frequency of use or movement of records, the value of records with regard to administrative, legal, fiscal, and historical interest, and the adequate and essential periods of retention and appropriate disposition of said records;

(2) Records set forth on the records retention schedule of a department shall be itemized, identified by form number if available, and by record title and record series title, in alphabetical or numerical sequence. For each record or record series, the schedule shall state the retention period for maintenance in the department involved as well as any City records center or centers utilized for the storage thereof. Original documents shall be listed separately from duplicate copies thereof. For each duplicate record, if such is not apparent from the face thereof, there shall be noted the location of the original record and the department having custody thereof; and

(3) Any record or record series contained in a records retention schedule shall be specifically and accurately described in accordance with guidelines developed by the City Clerk. The schedule shall also identify the physical form in which the record exists.

(b) **RECORDS CLASSIFICATION AND RETENTION TIME PERIODS.** The head of each department, or the authorized designee thereof, during the course of preparing for that department the records retention schedule or any amendment thereto, shall identify and designate each record or record series thereon according to one or more of the following classifications. Records which fall into more than one classification shall be retained for the longest applicable retention period.

(1) The following records shall be retained permanently:

- A. Historical records.
- B. Records affecting title to real property or liens thereon.
- C. Records required by Charter or statute to be retained.

D. Minutes, ordinances and resolutions by the City Council, Boards or Commissions.

(2) Vital records shall be retained, while current, subject to the provisions of Section 12.2 (b) (5) of this Code hereinabove.

(3) Retirement records shall be retained through the life of the employee, the life of that employee's surviving spouse, and throughout the dependency or the age of minority of the

employee's surviving children as provided in the Charter, plus five (5) years.

(4) Personnel, medical, hospital or similar records shall be retained until the date of termination of City employment plus five (5) years except that where termination is by retirement, records shall be retained for the same period of time required for those records in category 12.3 (b) (3) above.

(5) The following records shall be retained for a minimum of five (5) years unless a shorter or longer retention period is required by law or unless the record must be retained for a longer period of time to protect the City in the event of litigation:

A. Records exempt from public disclosure pursuant to provisions of the California Public Records Act, as amended.

B. Records related to any complaint of misconduct by the City or by any City officer or employee.

C. Records of a complaint to, or investigation conducted by, any City office or department for correctional, law enforcement, or licensing purposes.

D. Records used or customarily used in civil or criminal litigation, including any appellate review thereof.

E. Records prepared in connection with any claim filed against the City.

(6) Records not included in categories (1) through (5) or (7) and (8) of Subsection (b) shall be retained for a minimum of two (2) years unless a shorter period is otherwise permitted by law or a longer period is otherwise required by law, or unless, consistent with state law, a different period of retention is established by order or resolution of the Council. These records shall be identified and designated by form, series title, or by subject, listed either individually or by series, in alphabetical or numerical sequence.

(7) Records in the form of telephone and/or radio communications which are recorded routinely on a daily basis on tapes as a part of the regular public health, peace or safety operation of the Police and Fire Departments shall be retained for a minimum period of fifteen (15) months subject to the following provisions:

A. In the event that, prior to the date of destruction a record of this type (hereinafter referred to as "**tape record**") has been subpoenaed or ordered or requested to be held in connection with any litigation, either criminal or civil, or any administrative proceeding, or to the awareness of either the Los Angeles Police Department or Los Angeles Fire Department has otherwise become or is likely to become the subject of discovery proceedings in any of the above types of actions, a request for destruction thereof shall not be filed, nor shall the original of such tape record be destroyed unless:

(i) A re-recording or duplicate has been made of the conversation or other communication which is a part of the subject matter of the litigation or administrative proceeding contained on the original tape record;

(ii) The preparation of the re-recording or duplicate is or can be properly

authenticated;

(iii) The party or parties subpoenaing or otherwise ordering or requesting the production of the tape record have been advised of the intended destruction of the original tape record and that the retention of the original tape record may be requested; and

(iv) There has been no request for the retention of the original tape record as of the date the request for destruction is filed with the City Clerk.

In the event there is a request for retention of the original tape record, as distinguished from a re-recording or duplication thereof as above provided, the original tape record shall be retained until the litigation or administrative action is resolved or becomes final or there has been approval for the release of the record from the party or parties initially requesting the retention of such original tape record, provided that fifteen months have transpired since the original record was placed on the tape, and the Council has approved its destruction.

B. In the event the City Council, or a City officer or department, is informed or has reason to believe that a particular event, activity, or occurrence which took place may have been recorded either by the Police or Fire Department as part of a tape record, or part of such type of record of a particular date and that the record should be retained, the Council or such officer or department shall cause the department which has possession of the record to be informed that probable cause exists for retention of the record for reasons stated. Upon receipt of such notice, or based upon its own information or reason to believe that cause for retention may exist, the department in possession of the record shall review that portion of the tape or recording of the particular date or part thereof identified with respect to the event, activity or occurrence referred to. Upon completion of that review, if said department determines that the record contains matters identifiable under any of those Subsection (b) Categories (1) through (6), the record shall be retained for the longest period of time required by those categories under which identified.

(8) Records of latent fingerprints shall be retained in accordance with the following provisions:

A. For purposes herein the term "**latent fingerprint**" means any fingerprint (the tracing of physical characteristics of the lines upon a finger) that has been lifted from any object in order to identify the person or persons who have touched said object. The term "latent fingerprint" is not limited to a fingerprint that can be used only for positive identification purposes.

B. Latent fingerprints which have been lifted in connection with any action shall be retained until one year after such action has become final. An action shall include:

(i) a criminal investigation of a person or persons; or

(ii) a criminal prosecution of a person or persons whether or not the fingerprint has been introduced in evidence in the prosecution; or

(iii) a pending appeal or writ from a criminal prosecution; or

(iv) a civil proceeding or administrative adjudicatory proceeding related to the lifting of the latent fingerprint or to circumstances attendant thereto, and to any pending appeal or writ taken with respect thereto.

C. A latent fingerprint which is not directly related to a known pending action shall be maintained for a period of one year beyond the applicable statute of limitations in which an action could have been brought, but in no event shall a latent fingerprint be destroyed in less than three years from the date the latent fingerprint was lifted.

D. If a latent fingerprint related to an action for which there is no statute of limitations, it shall be kept for no less than 10 years from the date the latent fingerprint was lifted.

E. If a latent fingerprint affects or relates to more than one action, it shall be kept for one year beyond the statute of limitations applicable to the action with the longest such statute.

(c) **CERTIFICATION.** The head of each department, or the authorized designee thereof, shall certify that to the best of their knowledge, the descriptive titles, information, classification and designations on the records retention schedule, and any amendment thereof, meet City requirements with respect thereto, encompass all records of said department, and are correct.

(1) The City Clerk, when satisfied that all procedural and administrative requirements have been met, including vital and historical considerations, shall certify and transmit the departmental records retention schedules, and any proposed revisions to the City Attorney for review.

(2) The City Attorney, when satisfied that all legal requirements which may affect the retention or destruction of records have been met, including existing or potential litigation considerations, shall certify and return to the City Clerk the department records retention schedules, and any proposed revisions, along with any comments or recommendations for further revision.

(3) At the request of the City Attorney, department heads or authorized designees may be asked to review their departmental records retention schedules, and any proposed revisions, to insure that such schedules incorporate the determinations of the City Attorney with regard to legal and litigation requirements for the retention and destruction of records.

(4) Following the approvals of the City Clerk and the City Attorney, all records retention schedules and revisions to such schedules shall be returned to the City Clerk to be retained as the official records retention schedules for the City.

(d) **DUPLICATE RECORDS.** All duplicate records shall be listed as such on records retention schedules by each department or office, and may be destroyed, subject to the approval of the department head or the designated representative of such department head, if those records are no longer required to be retained in accordance with the retention periods established in said records retention schedules or their amendments.

SECTION HISTORY

Amended by: Subsec. (b), adds (13), Subsec. (d), renumbers Subdiv. (6) to Subdiv. (7), changes (12) to (13) in para. adds new Subdiv. (6), Ord. No. 167,699, Eff. 6-30-83; Subsec. (b), Subdiv. (14) added, Subsec. (d), Subdiv. (7) added, Ord. No. 161,778, Eff. 1-5-87; Subsec. (d), Subdiv. (8) added, Ord. No. 162,097, Eff. 4-26-87; In Entirety, Ord. No. 168,014, Eff. 7-27-92; Subsec. (c), Subdiv. (3), Subsec. (c), Subdiv. (4) Added, Subsec. (d), Ord. No. 171,472, Eff. 2-13-97.

**Sec. 12.4. Photographic And Electronic Reproduction.**

(a) **Conditions For Replacement of Original Records by Reproductions.** In the event records are reproduced in contemplation of the possible destruction, in accordance with the provisions of Section 12.5, of the original records so reproduced, the following conditions shall be met:

(1) All requirements of Government Code Section 34090.5 not specifically set forth in this subsection shall be complied with.

(2) The original record shall be photographed, microphotographed, or electronically or optically recorded by a procedure, and on a medium, that accurately captures an image of the record and does not permit additions, deletions or changes to the original document.

(3) The record shall be reproduced on a photographic film, optical disk or any other medium, provided the type of film, optical disk or other medium is in compliance with the standards or guidelines, or both, as recommended by the American National Standards Institute, referred to hereinafter as ANSI, the Association for Information and Image Management, hereinafter referred to as AIIM, or as required by California Government Code Section 34090.5 for archival recording of permanent records.

(4) The device used to reproduce the original record on film, optical disk or any other medium is one which accurately and legibly reproduces the original thereof in all details and does not permit additions, deletions or changes to the original document images. No page of any original records shall be destroyed if it cannot be reproduced with full legibility. The requirement of full legibility is met if the image on the photographic film is as legible as was the original document. In the case of digitally stored data, the requirement of full legibility is met if an eye-readable image produced from the data is as legible as was the original document. If the legibility of the original document is questionable, the fact should be recorded in the image or array of images, proximate to the record.

(5) The photographs, micrographics or other reproductions on film, optical disk or any other medium are made as accessible for public reference as the original records were. This accessibility shall include the provision of copies of records as required under Sections 12.30 through 12.33 of this Code.

(6) A true copy of archival quality of the film, optical disk or other medium of reproduction shall be kept in a safe and separate place for security purposes. The latter requirement shall be deemed satisfied if said copy is kept in a safe and separate place which meets the housing, environmental and inspection requirements of the most current ANSI and/or AIIM standards for archival storage conditions.

(7) Any reproduction of an original record pursuant to the provisions of this subsection shall be treated as a new original record. In that regard the records retention schedule for the department involved shall be amended to identify the reproduction as an original record.



(8) With respect to a photographic reproduction, the head of each department or office shall cause a certification to be prepared which states that:

- A. Provisions of this Code have been complied with.
- B. The original document is a record of the City of Los Angeles.
- C. The photographic reproduction is a true and correct copy of the original document.
- D. The photographic reproduction was made under the direction and control of the person signing the certification.
- E. The date on which the reproduction is being made.

Such certification shall be contained within the array of images of the photographic film or other medium of reproduction and shall be signed by the City employee responsible for supervision of the quality control of the film or by the corporate officer or manager of that entity performing the reproduction service who has the authority of the entity to so certify. If said certifying person is not a City officer or employee, then the City officer or employee regularly responsible for the work of photographic reproduction for the document involved shall certify as to the authority of such corporate officer or manager and include that certification in the image or array of images reproduced. If the photographic reproduction is done by a City agency, the City officer or employee signing the certification shall be a person regularly responsible for conducting and supervising a quality assurance program which includes routine resolution, density and archival stability testing in accordance with current industry standards of good practice.

If the photographic reproduction was done prior to the effective date of this Code section, a certification will be deemed sufficient if it certifies compliance with California Government Code Section 34090.5, as that section provided as of the date of the photographic reproduction, or other applicable law.

(9) Council approval shall be obtained as provided in Section 12.5 prior to any destruction of records from which photographic or electronic reproductions have been made.

(b) The Director of the Office of Administrative and Research Services shall adopt and issue rules and standards with respect to processes, procedures, equipment, media and storage relative to the photographic and electronic reproduction of City records for records retention and/or destruction purposes. These rules and standards shall apply only to reproductions made in contemplation of possible destruction of the original records and shall be developed in consultation with the City Clerk, the City Attorney, the City Engineer, the Information Technology Department and any other department or agency which the Director of the Office of Administrative and Research Services may deem helpful to assure, to the fullest extent feasible, the adoption of rules and standards that can be economically and efficiently implemented by the City and its departments.

The rules and standards shall provide, among other things, for the method of certifying that individual departmental and office facilities and procedures for the photographic and electronic storage of record images as sufficient to permit the destruction of original records in conformance with the requirements of this Code section.

Prior to any adoption thereof, proposed rules and standards shall be submitted to all affected City departments and offices for their review and said departments and offices shall have up to 30 days therefrom to comment and make recommendations with respect to the rules and standards proposed.

The rules and standards adopted shall reflect industry standards of good practice set forth by ANSI and/or AIIM or equivalent standard setting agencies.

**SECTION HISTORY**

Based on Ord. No. 132,902.

Amended by: In Entirety, Ord. No. 155,822, Eff. 10-24-81; Subsec. (c), Ord. No. 160,551, Eff. 1-9-86; In Entirety, Ord. No. 168,014, Eff. 7-27-92; Subsec. (b), First Para., Ord. No. 173,288, Eff. 6-26-00, Oper. 7-1-00.

**Sec. 12.5. Destruction of Records.**

**(a) ELIGIBILITY.**

(1) Unless otherwise provided herein or by other applicable law, no city department shall destroy, or cause or permit to be destroyed, any original record, as that term is defined in this chapter, without having first submitted a written request to the City Clerk and having received the written consent of the City Attorney and the approval of the City Council. Nor shall a department submit a request for such destruction of records without the head of that department having first made the following determinations:

- A. The record is under the management or control of said department head;
- B. Either records retention schedule minimum time limits have been satisfied, or photographic or electronic reproduction of the record has been made and the requirements of determination under Subdivision (2) below have been satisfied;
- C. Retention of the record is no longer required;
  - (i) For operations of that department, or
  - (ii) For operations of the City, or
  - (iii) To satisfy a City Council policy adopted by resolution, or a City Council request, or
  - (iv) By the City for any other reason of which the department head or authorized designee is aware; and
- D. The destruction of said record would not violate provisions of the State of California Government Code, Division 12 of this Code, or other applicable law.

(2) In the event the destruction of a record is under consideration, and copies thereof have been made by photographic or electronic reproduction as provided for in Section 12.4 of this Code, the head of the department or office involved shall also determine that:

A. At least two physically separate copies exist within the custody of the City, one which is of archival quality and one which is stored in accordance with Section 12.4 of this Code;

B. All conditions set forth in Section 12.4 of this Code and all standards and regulations otherwise adopted or required by law have been satisfied; and

C. The provisions of City Charter Section 434, where applicable, have been complied with.

(3) The head of the department requesting authority to destroy records, or the authorized designee, shall certify that determinations required in (2) immediately above have been made and that the statements set forth in such certification are true to the best of knowledge of said department head. No request for authority to destroy records shall be submitted to the City Clerk for transmittal to the City Council without such certification.

(4) At the termination of the applicable retention time for a record in the record category described in Section 12.3 (b) (7), the department head may submit a written request to the City Clerk for authority to destroy that record. The request shall include an identifying description of the date and time, extent and type of record on the tape, shall satisfy the requirements hereinabove, except those of Subdivisions (2) and (3), and be accompanied by a certification which verifies the completeness and accuracy of the description, and that the department head has no information from which to conclude that the record should be retained, and that said department head has made the determinations identified as A, B, C and D which are required in Subdivision (1) of this subsection.

(5) Upon receipt of a request of a department to destroy an original record, the City Clerk shall review the request to determine that all requirements have been met and shall certify that the record is not needed for historical purposes.

**(b) AUTHORITY TO SUBMIT.**

(1) The head of each department shall submit to the City Clerk, and shall thereafter cause to be kept current, exemplars of the signature of said department head and of the authorized designee thereof, if any, who shall have the current authority to submit and certify requests for authority to destroy records. The City Attorney shall cause to be submitted, and to be thereafter kept current, the exemplars of the signatures of those attorneys authorized to execute the consent of the City Attorney required by Government Code Section 34090.

The authority for, and authenticity of, such exemplars shall be identified and verified to the satisfaction of the City Clerk, and that officer shall maintain a current file and schedule of said signature exemplars, of the requests for destruction of records, and of the certifications submitted.

**(c) FORMS AND REPORTS.**

(1) Requests for authority to destroy records shall be submitted only on forms supplied by the City Clerk, or on computer generated reports approved by the City Clerk.

(2) All forms shall be completed to the satisfaction of the City Clerk by the department

head or authorized designee thereof requesting authority to destroy records.

(3) All forms and computer generated reports shall include at least the following information:

A. Description of the department and the division, bureau, office or unit thereof requesting destruction of records;

B. The record title or subject matter description of the records, or record series title, identified in the same manner as elsewhere in this chapter provided for records retention purposes;

C. The physical location of such records;

D. The quantity of such records;

E. The identification numbers of each box or container used to store said records where applicable;

F. Whether the records are originals or duplicates;

G. Dates of each record or inclusive dates of each record series listed for destruction; and

H. Date, job title and signature of the department head or authorized designee requesting the destruction of the records.

(4) The forms and/or computer generated reports shall also provide for, and when completed or produced shall include, or have attached thereto, the statements, verifications and certifications required hereinabove and the consent of the City Attorney.

(d) **PROCEDURE.** The head of each department has the primary responsibility to notify the City Council, in accordance with the following procedures, when records are available for destruction:

(1) Upon determination by the head of a department that destruction of certain records is appropriate, a request form or a computer generated report may be submitted through the City Clerk for authority to so proceed. The City Clerk may reject any request for authority to destroy records if more than six (6) months have elapsed from the date on which the head of the department involved, or the authorized designee thereof determined the eligibility of such records for destruction and so certified thereto. In such event the City Clerk may require new and current determinations and certifications to be prepared and submitted.

(2) All department requests and/or computer generated reports for authority to destroy records shall be accompanied by the certifications required herein and be presented through the City Clerk.

(3) The City Clerk shall review each request for authority to destroy records, and may remove from any list submitted for said purposes records or documents of historical importance, in order that they may be preserved, and to preclude their destruction. The City Clerk shall thereupon request the head of the department involved to physically deliver to the City Archives

the records so identified and removed from the records destruction request, provided, however, that if the record is only a Section 12.3 (b) category numbered (7) type record, that said record may be retained at the department, and the request for delivery to the City Clerk may be satisfied by delivery to the Clerk of a copy thereof in a form acceptable to the City Clerk for historical record purposes. Upon compliance with that request the Office of the City Clerk shall complete its processing of the previously submitted request for authority to destroy records as amended.

(4) When satisfied with the completeness, accuracy and adequacy of a submitted request for authority to destroy records, the City Clerk shall prepare the certification of that office to said effect. The City Clerk shall thereupon forward to the City Attorney the City Clerk's certification, together with the completed form or report requesting the destruction of records, the certification of the department head or the officer requesting said authority to destroy records, the City Clerk's findings, recommendations and comments thereon, if any, and the resolution proposed to be submitted to the City Council for its action.

(5) The City Attorney shall thereupon conduct whatever review of records that officer deems necessary in order to issue a written consent as required by law with respect to the request received for destruction of records. After consultation with the City Clerk and the head of the department involved, the City Attorney may recommend that a specific record or records be removed from that list of records which has been submitted as a request for authority to destroy records, that the request be so amended, and that said specific record or records be retained, notwithstanding time limitations provided on the records retention schedule involved. The written consent of the City Attorney, the departmental request for destruction of records, plus any findings and certifications with respect thereto and the proposed Council resolution of approval that said records be destroyed, shall be forwarded to the City Council by the City Attorney. In the event the written consent of the City Attorney does not apply to all records listed on the final resolution and/or the request for authority to destroy records which is submitted to the City Council, any such records to which the consent does not apply, but which have not been deleted from the list, shall be identified as records the destruction of which is not consented to by the City Attorney, and said officer, or the authorized designee thereof as in this chapter provided, shall also attach thereto the reasons for any such lack of consent.

(6) The Office of the City Attorney shall return to the Clerk, under separate cover for appropriate disposition, any material which the City Attorney does not forward to the City Council.

(e) **APPROVAL.** The City Council may approve, conditionally approve, or disapprove, either in whole or in part, the destruction of those records to which the consent of the City Attorney applies and which appear on the destruction of records request submitted to the Council. The determination and action of the City Council shall thereafter be implemented by the City Clerk, or in the event the record involved is identified as a Section 12.3 (b) category (7) type record, then the department head shall cause such implementation to take place.

#### SECTION HISTORY

Based on Ord. No. 132,902.

Amended by: In Entirety, Ord. No. 155,822, Eff. 10-24-81; Subsec. (a), adds (4) Subsec. (d), 2nd sentence of Subdiv. (4), Subsec. (e), last sentence, Ord. No. 157,699, Eff. 6-30-83; In Entirety, Ord. No. 168,014, Eff. 7-27-92.

**Sec. 12.6. Use of Descriptive Terms.**

Terms used as record titles, classifications, categories, or as descriptions of files on a records retention schedule or any amendment thereto, or on any request for destruction of records or any form or computer generated report applicable to either, shall be descriptive. They shall not include the use of the word "miscellaneous" or "various", or words of similar connotation, nor shall any such schedule or request bearing such nomenclature be submitted to the City Council for its consideration.

SECTION HISTORY

Based on Ord. No. 132,902.

Amended by: In Entirety, Ord. No. 155,822, Eff. 10-24-81; In Entirety, Ord. No. 168,014, Eff. 7-27-92.

**Sec. 12.7. Applicability of the Chapter.**

The provisions of this chapter shall apply to all departments whose funds, in whole or in part, are provided for in the General City Budget. It is the intent of the City Council that departments using other funds shall also comply with the provisions of this chapter. All departments shall comply with applicable law.

SECTION HISTORY

Added by Ord. No. 155,822, Eff. 10-24-81.

Amended by: In Entirety, Ord. No. 168,014, Eff. 7-27-92.

**MEMORANDUM OF UNDERSTANDING**  
**BETWEEN THE**  
**CITY OF LOS ANGELES**  
**AND THE**  
**UNIVERSITY OF SOUTHERN CALIFORNIA**

This Memorandum of Understanding (MOU) is entered into pursuant to the provisions of Section 830.7(b) of the Penal Code, Section 67381 of the Education Code, and Section 1808.25 of the Vehicle Code, in an effort to provide the University of Southern California (USC) the authority, allowed by law, to maintain order and ensure the safety of those individuals employed on, attending school at, or visiting, the USC campus. The MOU also reserves the right of the City to regulate and monitor the activities of any entity designated to restrict its citizens through the use of the powers granted herein.

Penal Code Section 830.7(b) authorizes the Chief of the Los Angeles Police Department (herein after referred to as the "Chief of Police") to allow, persons not peace officers, but regularly employed as security officers for independent institutions of higher education recognized under subdivision (b) of Section 66010 of the Education Code, the authority to exercise the powers of arrest of a peace officer as specified in Penal Code Section 836 during the course and within the scope of their employment.

Education Code Section 67381 requires local law enforcement agencies to enter into written agreements with campus law enforcement agencies, including those campus security services with an MOU pursuant to Penal Code Section 830.7(b), for the purpose of designating which agency shall have operational responsibility for the investigation of each Part I violent crime and to delineate the specific geographical boundaries of each agency's operational responsibility.

Vehicle Code Section 1808.25 authorizes the enforcement of Parking Restrictions by nonprofit independent institutions of higher education incorporated in this State if specifically authorized to do so in a Memorandum of Understanding authorized by Penal Code Section 830.7.

**ARTICLE 1-PARTIES**

This MOU is entered into by and between the City of Los Angeles ("City") acting by and through the Chief of Police ("Chief of Police"), Los Angeles Police Department (LAPD) and USC acting by and through the senior Vice President, Administration, University of Southern California ("USC" or "University of Southern California").

**ARTICLE 2-TERM**

The term of this MOU shall commence on October 1, 2009 at 12:01 a.m. and shall expire at 11:59 p.m. on October 1, 2010. Unless, written notice is provided by one party to the other of non-extension of this MOU at least thirty (30) days prior to October 1, 2010, this MOU shall

be automatically extended for one year terms commencing September 1, 2009, subject to the same terms and conditions as the initial term, unless at least (30) days prior to the expiration of any one year extension, either party to this MOU gives to the other party written notice of termination effective as the expiration of that current one year term. Notwithstanding the above, either party may terminate this MOU with thirty (30) days written notice.

### ARTICLE 3-AUTHORITY

#### (A) ARREST POWERS

It is the intent of the Chief of Police, by entering into this MOU, to allow employees of the USC Department of Public Safety (DPS) to exercise the arrest powers described in Penal Code Section 830.7(b). In doing so, the Chief of Police recognizes that this authority is one normally restricted to peace officers whose activities are closely monitored and controlled by established laws, policies, and procedures. By allowing USC DPS personnel this authority, it is expected that the regulatory procedures outlined in this MOU be strictly followed.

This MOU is not intended to designate USC DPS personnel as agents of the City of Los Angeles, nor is it intended to provide USC DPS personnel with any peace officer or public official status or any other peace officer authority or power other than the proscribed powers of arrest per Penal Code Section 836, which generally allow arrests based on probable cause. Anyone arrested by USC DPS personnel shall, without unnecessary delay, be transported by DPS or an assigned LAPD USC officer to the appropriate LAPD booking facility for review, evaluation, and when appropriate, booking advice and approval. Such approval can only be granted by the concerned on-duty LAPD Watch Commander. If necessary, the processing of felony arrestees will be facilitated through the assistance of an LAPD sworn police officer. In the case of an arrest of an adult misdemeanant who meets the criteria for a Release from Custody (RFC), established LAPD guidelines shall be followed.

**Note:** Completion of RFCs by DPS personnel will generally be completed, but not necessary limited to Intoxication, LAMC 41.27, 25620 of the Business and Professions code and the Loud Party Ordinances, 41.57 and 41.58 LAMC. Any requests to cite additional sections shall be with the approval of the Chief of Police.

If any evidence is obtained during the course of an arrest, the concerned DPS officer shall ensure it is properly booked without unnecessary delay in accordance with established LAPD guidelines. The on-duty Watch Commander of the LAPD booking facility shall review the concerned property report completed by the booking DPS personnel.



In cases where an arrestee has a medical condition that can be treated by an LAPD Jail Dispensary, it will be the responsibility of the USC DPS personnel to transport and process the arrestee to such a facility at the direction of the LAPD Watch Commander. For arrestees that require medical attention and treatment at a non-jail facility, the responsibility will remain with the LAPD Watch Commander to approve continued detention based on the seriousness of the offense. Security of the hospitalized arrestee will be provided as sanctioned by current LAPD guidelines. The on-duty Watch Commander for the Area of occurrence shall approve all related reports, regardless of the booking location.

**Note:** The Miranda Advisement is generally only necessary for in-custody interrogations by peace officers; therefore, to eliminate any misunderstandings within the judicial or investigative process, USC DPS personnel shall not provide arrestee with the Miranda advisement nor take any statements.

(B) ISSUANCE OF PERSONAL SERVICE CITATIONS

Pursuant to Vehicle Code Section 1808.25, USC DPS personnel are hereby authorized to enforce parking restrictions, issue personal service citations to pedestrians and bicyclists as allowed by the Penal Code Section 830.7(b), within the boundaries of the campuses, as identified as University Park Campus and Health Sciences Campus (together, the "Campus") in Exhibit A, attached hereto and incorporated herein by this reference. Based on the requirements set forth in the California Vehicle Code (CVC), USC DPS personnel shall not issue personal service citations to motorists in or outside of the above-captioned boundaries. Additionally, as outlined in Section 21055 of the CVC and LAPD policy, USC DPS personnel are not authorized to initiate vehicle pursuits for any reason.

(C) FOLLOW-UP INVESTIGATIONS

The Chief of Police has determined, in accordance with Section 67381 of the Education Code, that it is in the best interest of the City for the LAPD to maintain the primary investigative responsibility and authority for all Part I violent crimes occurring on and around the USC campus or on property owned or controlled by USC within the City of Los Angeles.

The LAPD will assign a Detective to manage and/ or conduct follow-up investigations on crimes reported on the USC campus or property owned or controlled by USC. Any reportable incidents as defined in Article 5 (b) shall remain the investigative responsibility of the concerned LAPD investigative entity as determined by the LAPD Southwest (SW) Area Commanding Officer. Although it is the intent of the LAPD to assign the aforementioned Detective for the purposes identified in this MOU, nothing shall preclude the Chief of Police from reassigning the Detective to other duties based upon the authority granted him in the Los Angeles City Charter, as he deems said reassignment necessary.

(D) ACCESS TO LAPD COMMUNICATIONS

In accordance with established LAPD procedures, specifically trained USC DPS staff will be allowed access to LAPD's communication system to be used only for official police communications. Such communications will be limited to initial and supplemental broadcasts of emergency crime information. Additionally, only when access to LAPD personnel are unavailable, authority is granted to select DPS staff to request a clear frequency to check a suspect for wants and/or warrants.

**Note:** Select DPS staff is defined as DPS personnel identified by the Chief of Public Safety, DPS or his/her designee, and agreed to by the Commanding Officer (CO), SW Area to be allowed access. Selected DPS staff would receive the requisite training provided by the SW Area Training Coordinator.

(E) DEFINED GEOGRAPHIC AREA OF RESPONSIBILITY

The authority granted USC DPS personnel under this MOU shall be restricted to the areas as identified in Exhibit A with respect to the University Park Campus and the Health Sciences Campus and those properties outside the defined areas on Exhibit A which are owned or leased by USC, when the property is used for the primary purpose of; housing USC employees, students, faculty or guests; parking vehicles for USC employees, students, faculty, or guests; providing a location for students, faculty, or guests to meet, study, or receive classroom instruction; or any other facilities within the City when being used for the purpose of conducting USC sponsored athletic events, i.e. Los Angeles Memorial Coliseum and Sports Arena (collectively, the "Geographic Area of Responsibility").

**Note:** The authority granted under this MOU does not extend to public thoroughfares outside the defined USC Campus or to other properties owned or leased by USC which are either commercial or residential and area generally available for use by the public.

**ARTICLE 4-AUTHORIZED ASSIGNMENT AS LIMITATION ON POWER OF ARREST**

In accordance with the provision of 830.7 (b) of the California Penal Code, duly authorized USC DPS personnel shall be vested with powers of arrest per Penal Code Section 836 only while they are on-duty with the USC DPS, performing "authorized assignment" within the defined Geographic Area of Responsibility and, unless on Campus (as defined), personnel shall wear an approved uniform which identifies the wearer as a USC DPS employee.

## ARTICLE 5-REPORTING INCIDENTS, WRITTEN REPORTS, RECORDS, AND INSPECTIONS

The proper recording of information and exchanging information is critical to the process of deploying resources both inside and outside the university. There is also a need for compatible record keeping and UCR reporting. This reporting requirement is further identified in the following paragraphs:

- (A) USC Administration upon becoming aware of a significant incident occurring within the defined Geographic Area of Responsibility shall notify, without unnecessary delay, the USC DPS and/or LAPD. A significant incident is defined as an act or omission to act which would constitute a felony or misdemeanor under California law or any other incident of a sensitive public safety or hazardous nature.

Note: A "significant incident" is defined as an act or omission to act which would constitute a felony or misdemeanor under California law or any other incident of a sensitive public safety or hazardous nature.

- (B) The USC DPS, upon becoming aware of a significant incident, shall complete the appropriate crime report(s), and without unnecessary delay submit the report(s) to the on-duty Southwest Watch Commander, or if outside Southwest Area, the Area of occurrence, for approval. Upon completion and approval, a copy of each crime report and/or arrest report or RFC completed by USC DPS personnel shall be forwarded to the Southwest Detective Division Commanding Officer without unnecessary delay. In those cases where the incident constitutes a complex felony under California law or a crime of violence involving the use of a weapon, or a reportable incident as defined below, USC shall immediately notify the Watch Commander of the appropriate patrol division where the incident occurred.

Note: USC DPS personnel shall not conduct either the preliminary or follow-up investigations of any "reportable incident" described below. In those instances, immediate notification shall be made to the Southwest Area Patrol Watch Commander or depending on the emergent circumstances, any on-duty, sworn LAPD personnel.

A reportable incident shall include but not be limited to the following:

- Homicide
- All crimes where shots were fired
- Sexual assaults (see below)
- Bomb threats
- Crimes or incidents which are motivated by hatred due to race, religion, or ethnic group
- Injuries where City liability may be an issue
- Suicides and attempt suicides

- Hazardous material spills or contamination
- Theft over \$5,000.00
- Incidents that if known would be considered newsworthy or could have a significant impact on the City of Los Angeles.
- Any incident in which the LAPD determines to be in the best interest of the City of Los Angeles to handle.

#### Sexual Assault Reporting

The crime of rape, or attempted rape, is a serious criminal act, which requires the immediate investigation by LAPD uniformed or detective personnel. While it is understood that some victims may be hesitant or reluctant to cooperate in the investigation of these crimes, it is imperative that a preliminary investigation be conducted to identify, if possible, the involved suspect(s). Rape is a crime of violence and suspects who commit this type of violent act often are repeat offenders. There is an inherent obligation to try to prevent future occurrences.

The term sexual assault is intended to include those criminal acts described in the California Penal Code and the California Welfare and Institutions Code. It includes the crimes of rape, attempted rape, sodomy, oral copulation, indecent exposure, and child molestation. Whenever a crime of a sexual nature is reported to USC DPS [security] personnel, notification shall immediately be made to the appropriate geographic area Watch Commander who will make the appropriate detective notifications. While the first concern shall be for the well being and medical treatment of the victim, the reporting of the incidents to LAPD personnel shall not be delayed because of such treatment or request for such treatment. The reluctance of the victim to report the crime, identify the suspect(s), or proceed with the prosecution shall not be a factor in the reporting policy of USC DPS personnel.

In no instance shall the victim of a sexual crime be counseled, persuaded, advised, or encouraged by any USC DPS personnel not to report the crime. USC DPS personnel shall immediately contact their Watch Commander upon learning of a sexual assault crime, and the Watch Commander shall immediately notify the concerned LAPD geographic area Watch Commander.

- (C) The USC DPS will maintain a Daily Occurrence Report, recording all incoming calls and significant incidents relating to police activity. A copy of the report for the University Park campus shall be forwarded to the CO, SW Area. A copy of the report for the Health Science campus shall be forwarded to the CO, Hollenbeck Area. The report shall be forwarded within 24 hours after the completion of the period covered by the report.

- (D) Any general orders issued by USC DPS pertaining to USC response to, or reporting of crimes will be made available upon request to the CO, SW Area for appropriate LAPD review and approval.
- (E) All report forms used by the USC DPS for the reporting of crimes shall be submitted to the Chief of Police for approval, to insure compatibility with the Los Angeles Police Department's report forms.
- (F) Weekly crime statistics shall be maintained and supplied to SW Detective Division by USC DPS depicting specific locations of reported crimes on the campus.
- (G) During the term of this MOU, USC shall immediately report all discharges of firearms, (accidental, negligent, or intentional) involving USC DPS personnel to the LAPD and cooperate, as required, with the investigation of the firearms incidents conducted by the LAPD. The LAPD will investigate the criminal aspects of a firearm discharge. The USC DPS will be responsible for administrative matters associated with the discharge of firearms.
- (H) All records and files of enforcement activities granted by this MOU to USC personnel shall be open for inspection to designated members of the LAPD.
- (I) All records of complaints or investigations of complaints lodged against USC DPS personnel arising from the exercise of authority granted by this MOU shall be open for inspection and when necessary investigation by designated members of the Los Angeles Police Department.
- (J) USC DPS shall submit monthly rosters of all scheduled duty assignments of all security officers one month in advance of the scheduled assignments to the concerned Area commands. Said roster shall be submitted no later than the fifth day of the concerned month.
- (K) USC DPS shall submit monthly reports to the concerned Area commands on the activities of officers at USC pertaining to the exercise of power granted by this MOU.
- (L) Follow-up investigations for crimes occurring within the City shall be the sole responsibility of the LAPD (LAPD Manual Section 4/810) and not performed without the knowledge of the Department.

**Note:** No administrative type interviews shall be conducted by USC personnel of any known party of a crime identified as the person reporting, victim, suspect, or witness, without the prior approval of the assigned LAPD detective.

- (M) Any use of force by USC DPS personnel related to the authority granted by this MOU shall be documented and explained under the heading of "Use of Force" in the appropriate report (i.e. Arrest Report, Crime Report, USC Daily Occurrence Report).
- (N) It is agreed that all SWAT, hostage, and/or tactical incidents, as well as narcotic and vice investigations are the exclusive domain of the LAPD.

Note: All of the above described reports, statistics, and records shall be provided unless otherwise agreed to by the LAPD.

#### **ARTICLE 6-ACCESS TO POLICE DEPARTMENT AND CRIMINAL OFFENDER FILES**

Most law enforcement related information accessible through the LAPD automated systems is confidential and restricted to viewing by police agencies and their authorized employees. The California Public Records Act restricts access to the information contained within crime reports and arrest reports. The basic criterion for release of information from an arrest report is limited to the first nine lines. Release of crime report information is limited to the victim, their authorized representative, an insurer, or a party experiencing a loss during the crime.

University of Southern California personnel shall be restricted to accessing only that information from Federal, State, City, or LAPD records or files, as authorized by law, which limits USC access to those records available to the general public. USC shall not maintain files of LAPD reports. For purposes of this MOU, an LAPD report is defined as any report requiring the issuance of an LAPD Division of Records file number (DR Number).

To ensure compliance with all Los Angeles Police Department mandates, and internal tracking systems, USC public safety officers will be entered into the Training Management System, and issued serial numbers. This will ensure Consent Decree compliance and departmental goals.

Statistical crime information for the USC campus and the surrounding reporting districts will be provided by LAPD upon receiving a request from authorized USC personnel.

#### **ARTICLE 7-PRIVATE SECURITY SERVICE ACT**

The State of California (State) Legislature has established that the public should be able to easily distinguish between security services personnel and local law enforcement personnel. In enacting the legislation regulating private security services, the State had included armed personnel of agencies such as the USC DPS campus security. To ensure the safety of the public and in furtherance of this legislation USC and USC personnel provided with authority by this MOU shall comply with all applicable California Business and Professions Code (BPS) Sections.

## **ARTICLE 8-PROVISIONS OF LAW AND SEPARABILITY**

The parties agree that this MOU is subject to all current and future applicable Federal, State, and local laws, the City Charter, and any lawful rules and regulations enacted by independent commission of the City. If any Article, part, or provision of this MOU is in conflict or inconsistent with such applicable provisions of Federal, State, or local laws, or the Charter of the City of Los Angeles, or rules and regulations enacted by independent City commissions, or is otherwise held to be invalid or unenforceable by any court of competent jurisdiction, such Article, part, or provision shall be suspended and superseded by such applicable law, or regulations, and the remainder of this MOU shall not be affected thereby.

## **ARTICLE 9-QUALIFICATION AND TRAINING STANDARDS OF USC DEPARTMENT OF PUBLIC SAFETY**

In order to be granted the powers of arrest as specified in Section 836 PC, personnel employed by USC DPS must comply with all of the following requirements:

- (A) Be regularly employed full-time by the University of Southern California, Department of Public Safety as a full-time public safety officer in good standing;
- (B) Meet the minimum standards prescribed by the Commission on Peace Officer Standards and Training (POST) as set forth in Section 832 PC;
- (C) Meet such further reasonable qualifications for employment deemed necessary by the Chief of Police, Los Angeles Police Department;
- (D) Be included on a roster of those public safety personnel authorized by the Chief, Department of Public Safety, University of Southern California, to make arrest in the circumstances specified in Section 836 PC.
- (E) Armed DPS staff as required by mutual agreement will be allowed to participate in firearms qualification on LAPD sanctioned ranges. Qualification standards for DPS will be in accordance with POST requirements.
- (F) Training provided by LAPD for DPS and/or joint training for both LAPD SW and DPS will follow existing LAPD protocol. Initial requests will be reviewed and evaluated by the CO, SW Area prior to approval of the CO, Operations-South Bureau and the CO of LAPD's Training Group.

## **ARTICLE 10-INSURANCE**

As a part of liability and indemnification concerns related to this agreement, the following information and agreement are made:

- (A) USC shall procure at its expense, and keep in effect at all times during the term of this MOU, the types and amount of insurance specified in Addendum 1 hereof. The specified insurance (except for Workers' Compensation and Employer's Liability) shall also, wither by provisions in the policies, by the City's won endorsement form, or by other endorsement attached to such policies, include and insure the City, its Police Department, its Board of Police Commissioners, all of the City's officers, employees, and agents, their successors and assigns, and of other non-USC facilities identified within this MOU, against the areas of risk described in Addendum No. 1 hereof arising out of the acts or omissions of the officers, employees, or agents of USC in its operations or other functions related to the authority granted by the terms of this MOU.
- (B) Each specified insurance policy (other than Workers' compensation and Employer's Liability) shall contain a contractual enforcement which shall state, "Such insurance as is afforded by this policy shall also apply to liability assumed by the insured under the MOU between the insured and the Chief of Police, City of Los Angeles, pursuant to the provisions of Section 830.7(b) PC."

All such insurance shall be primary and non-contributing with any other insurance held by the City or City's Police Department, or other non-USC organizations, where liability arises out of, or results from, the acts or omissions of USC, its agents, employees, officers, assigns, or any person or entity acting for or on behalf of USC. Such policies may provide for reasonable deductible and/or retention's based upon the nature of USC's operations and the type of insurance involved.

- (C) The City shall have no liability for any premiums charged for such coverage(s). The inclusions of the City, its Police Department, its Board of Police Commissions, and all of the City's officers, employees, and agents, and their agents and assigns, or other non-USC organizations owning facilities identified in this MOU, as insured is not intended to, and shall not, make them, or any of them, a partner or joint venture with USC in USC's operations pursuant to this MOU. Upon failure of USC to provide and maintain the insurance required herein after ten (10) days written notice to comply, the City may (but shall not be required to) procure such insurance for USC to protect the City's interest and USC agrees to reimburse the City fully to cover such expense.
- (D) USC shall provide proof of all specified insurance and related requirement to the City either by production of the actual insurance policy (ies) or by use of the City's own endorsement form(s). The University of Southern California shall not be authorized by the provisions of 830.7(b) PC and shall not commence activity pursuant to this MOU until the documents evidencing all specified coverage have been filed with the City. The documents shall contain the applicable policy number(s), the inclusive dates of policy coverage, and the insurance carrier's name shall bear an original signature of an authorized representative of said carrier: and shall provide that such insurance shall not be subject to cancellation,



reduction in coverage, or nonrenewable except after written notice by certified mail, return receipt required, to the City Attorney of the City of Los Angeles at least thirty (30) days prior to the effective date thereof. They shall be reviewed by and be subject to the approval of the City Attorney for conformity to legal requirements. The City reserves the right to have submitted to it, upon request, all pertinent information about the agent and carrier providing such insurance.

The Workers' Compensation/Employer's Liability exposure may be self-insured when the program has been authorized by the State. Evidence of self-insured Workers' Compensation/Employer's Liability program shall be a copy of the certification authorizing the self-insured program.

#### **ARTICLE 11-ATTORNEY'S FEES**

If the City, including its Board of Police Commissioners, and the City's officers, agents, servants and employees, or any other non-USC organization, without fault, shall be made a party to any litigation commenced by or against USC arising out of the authority granted pursuant to the terms and provisions of this MOU; and as a result of which USC is finally adjudicated to be liable, then USC shall pay all costs, expenses, and reasonable attorney's fees incurred by or imposed upon the City or any other organization in connection with such litigation. In any action by the City, the LAPD, the Chief of Police, or USC for the recovery of any sum required to enforce any of the terms, covenants, or conditions contained herein, the prevailing party shall be entitled to reasonable attorney's fees in addition to cost, expenses, and necessary disbursements incurred in such action. Each party shall give prompt notice to the other of any claim or suit instituted against it that may affect the other party.

#### **ARTICLE 12-CITY INDEMNIFIED AND HELD HARMLESS BY USC**

In addition to the provisions of Addendum No. 1, herein, USC shall fully indemnify, defend, and keep and hold the City, including its Board of Police Commissioners, the City's officers, agents, servants, and employees, harmless from any and all costs, liability, damage, or expense (including costs of suits and fees and reasonable expenses of legal services) claimed by anyone by reason of injury to or death of persons, or damage to or destruction of property, including property of USC, sustained in, on or about the premises designated in this MOU or arising out of USC's use or occupancy thereof, or as a proximate result of the acts or omissions of/or by USC, its agents, servants, or employees to act as required by this MOU. It is the intent of the parties of this MOU that the City, its officers, employees, agents, and assigns, or any other non-USC organization, shall have no financial liability or obligation resulting from any acts or omissions to act as required by this MOU by USC, its officers, employees, agents, and assignees in connection with the activities authorized by this MOU. And that if there is during the term of the MOU any such financial liability or obligation, USC shall be fully and solely responsible therefore as between the parties of this MOU.

## ARTICLE 13-NOTICE

Written notices to the City, the Chief of Police, and to the City Attorney of the City of Los Angeles shall be given by registered or certified mail, postage prepaid, and addressed to said parties at Los Angeles City Hall, 200 North Spring Street, Los Angeles, California, 90012, or to such other addressee as these parties may designate by written notice to USC. Written notices to USC shall be given by registered or certified mail, postage prepaid, and addressed to, University of Southern California, University Park, Los Angeles, California, 90089-0011, or to such other addressee as USC may designate by written notice to the Los Angeles Police Department. Notwithstanding the foregoing, all notices may be delivered personally to the Chief of Police, the Office of the City Attorney, or to the University of Southern California.

## ARTICLE 14 - LAPD STAFFING, FUNDING, FACILITIES AND EQUIPMENT

By July 1, 2008, and annually thereafter, LAPD agrees to provide USC with the deployment of sworn personnel and the staffing level to be determined by the Chief of Police. On the direction of the Chief of Police, or his designee, the staffing level of assigned personnel can be modified in response to critical incidents or staffing shortages in response to public safety.

During the assignment of sworn LAPD officers to the defined geographic area of responsibility covered by DPS, the LAPD agrees to provide basic patrol functions, along with limited investigative services consistent with the afore-mentioned guidelines. The services include, but are not limited to: response to radio calls for service; assistance with crowd and traffic control during labor disputes and student protests; suppress criminal activity through visible and surreptitious enforcement; conduct vehicular and pedestrian traffic control in the defined area; conduct community meetings which include and are not limited to crime prevention and education seminars; and, limited investigative follow-ups as defined in Article 3, subsection C.

### (A) LAPD STAFFING

Minimum staffing of assigned sworn LAPD officers will include: (1) Detective; (1) Senior Lead Officer, Police Officer 3+1; and (4) Police Officers II. The assigned LAPD sworn personnel would be under the Southwest Area's chain of command and direction. Southwest Area would effectively monitor the deployment, mission, and supervision of the assigned staff.

### (B) EQUIPMENT

USC agrees to the purchase of the following items:

1. Two Vehicle License Plate Recognition (VLPR) units to be installed in three LAPD marked units assigned to SW Officers assigned as dedicated USC resources in the defined USC Response Area.

2. Two LAPD Local Area Network computer terminals to be installed in an area so designated by USC DPS for the sole use by LAPD SW personnel.
3. Ten portable LAPD radios.

(C) FACILITIES

The USC DPS agree to designate an area(s) for the assigned LAPD SW personnel to co-locate with DPS personnel.

(D) REPORTING

LAPD shall provide USC with a quarterly report of the activities performed by the LAPD SW USC personnel assigned to full time duties at USC. This report will reflect actual number of days worked at USC, significant events or activities, any arrests associated with the VLPR equipped vehicles, and current crime statistics.

IN WITNESS WHEREOF, the parties hereto have caused this Memorandum of Agreement to be executed by their duly authorized officers as set forth herein below:

**UNIVERSITY OF SOUTHERN CALIFORNIA**

  
\_\_\_\_\_

TODD DICKEY  
Senior Vice President, Administration

Date 10/20/09

**LOS ANGELES POLICE DEPARTMENT**

  
\_\_\_\_\_

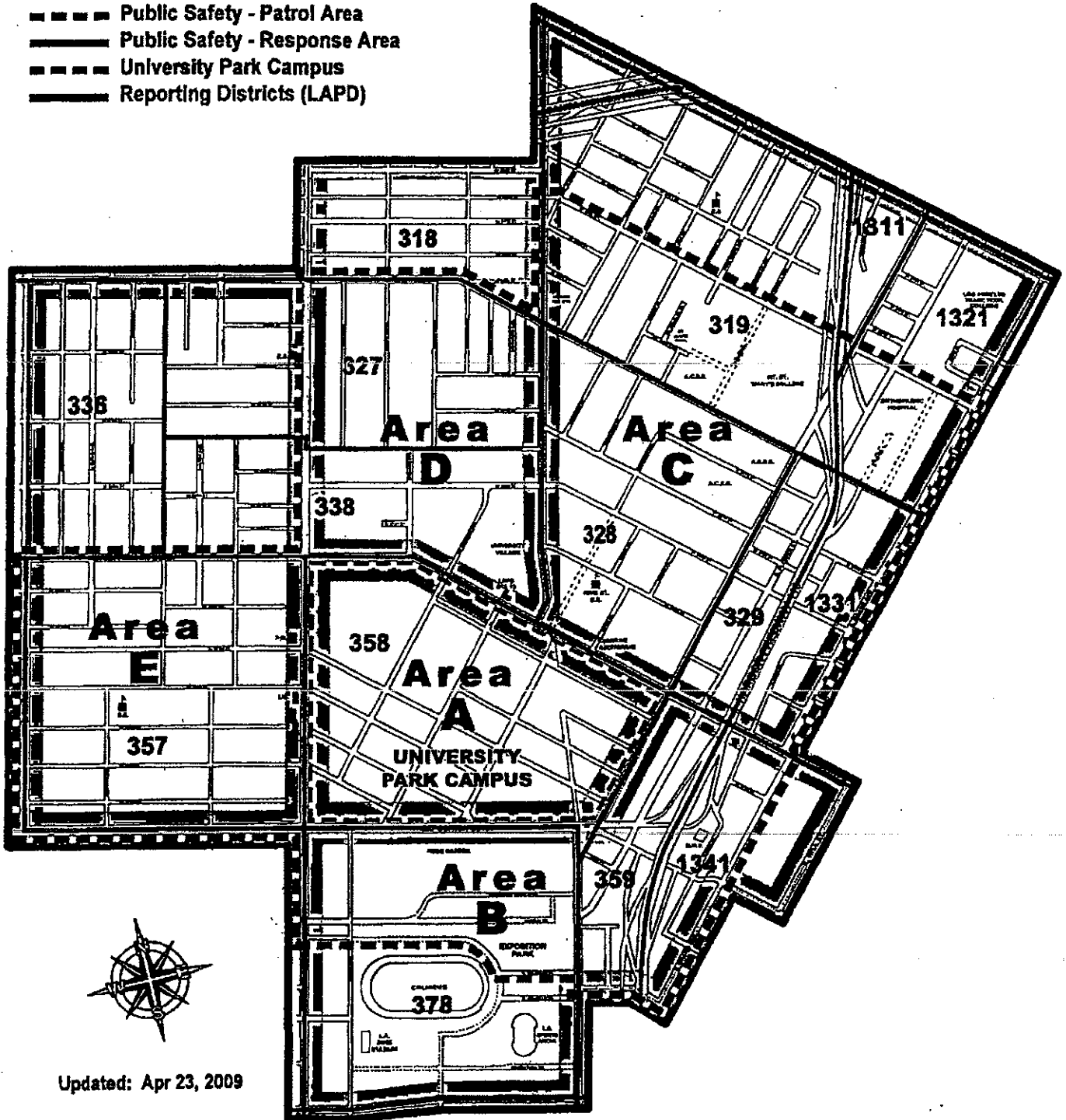
WILLIAM J. BRATTON  
Chief of Police

Date 10/19/09

# UNIVERSITY PARK CAMPUS

## Patrol and Response Boundaries





- Public Safety - Patrol Area
- Public Safety - Response Area
- University Park Campus
- Reporting Districts (LAPD)

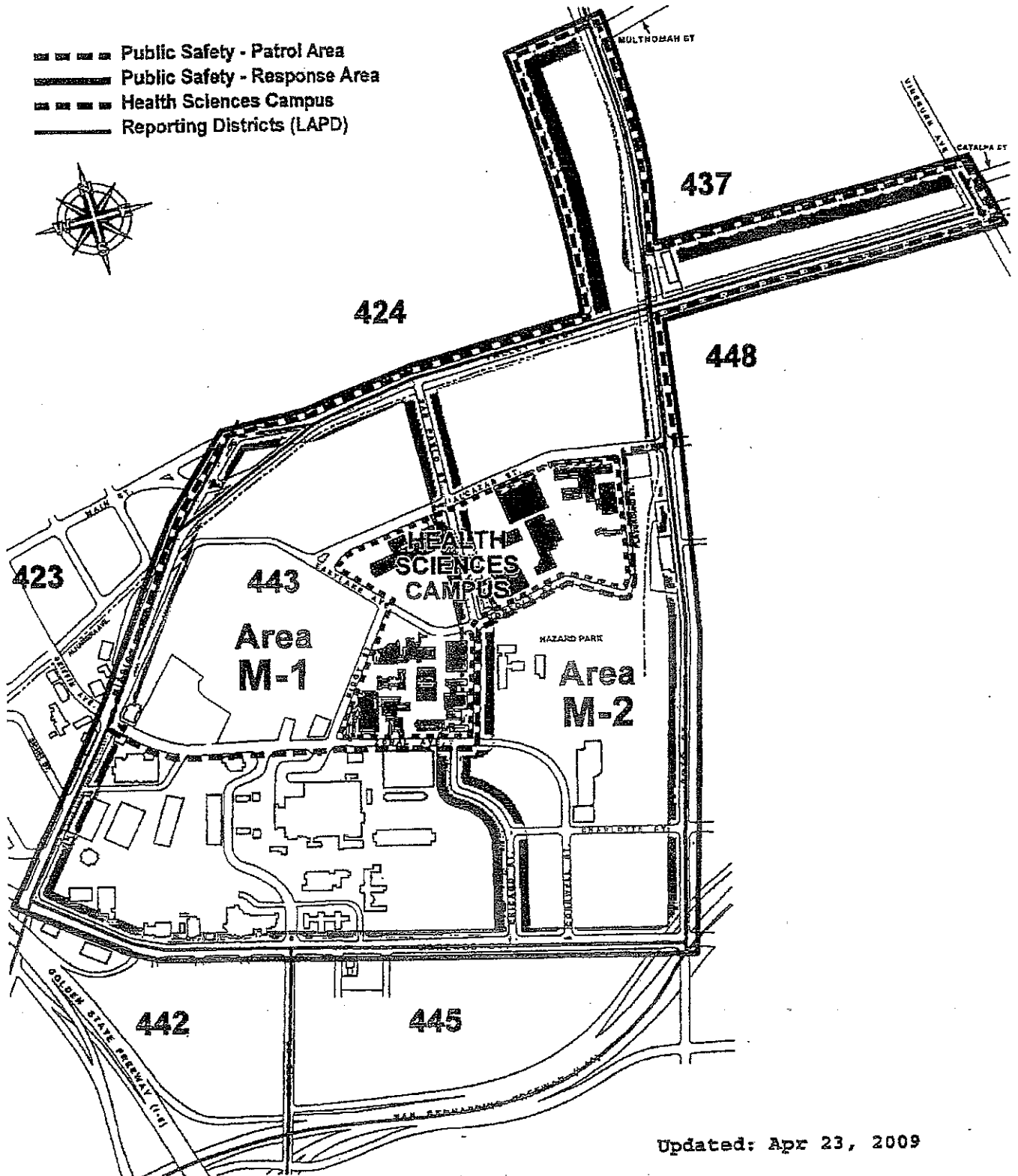


Updated: Apr 23, 2009

# HEALTH SCIENCES CAMPUS

## Patrol and Response Boundaries

-  Public Safety - Patrol Area
-  Public Safety - Response Area
-  Health Sciences Campus
-  Reporting Districts (LAPD)



Updated: Apr 23, 2009

# ACORD CERTIFICATE OF LIABILITY INSURANCE

OP ID G2  
UNIVE-5

DATE (MM/DD/YYYY)  
08/01/08

**PRODUCER**  
Arthur J. Gallagher & Co.  
Ins Brokers of CA Inc. 0726293  
505 N.Brand Blvd, Suite 600  
Glandala CA 91203-3944  
Phone: 818-539-2300 Fax: 818-539-2301

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW.

**INSURED**  
University of So. California  
Attn: Jim Anderson  
851 Downey Way HSH 300  
Los Angeles CA 90089-1058

INSURERS AFFORDING COVERAGE	NAIC #
INSURER A: <b>United Educators Insurance</b>	
INSURER B: Natl. Union Fire Ins Co of PA	19445
INSURER C:	
INSURER D:	
INSURER E:	

## COVERAGES

THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. AGGREGATE LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

TYPE OF INSURANCE	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS
<b>A</b> <input checked="" type="checkbox"/> <b>GENERAL LIABILITY</b> <input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS MADE <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> \$2MM SIR applies GENL AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC	[REDACTED]	06/01/08	05/01/09	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (EA OCCURRENCE) \$N/A MED EXP (Any one person) \$N/A PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMP/CP AGG \$2,000,000
<input checked="" type="checkbox"/> <b>AUTOMOBILE LIABILITY</b> <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS <input checked="" type="checkbox"/> \$2MM SIR applies	[REDACTED]	06/01/08	05/01/09	COMBINED SINGLE LIMIT (EA ACCIDENT) \$1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
<input type="checkbox"/> <b>GARAGE LIABILITY</b> <input type="checkbox"/> ANY AUTO				AUTO ONLY - EA ACCIDENT \$ OTHER THAN AUTO ONLY: EA ACC \$ AGG \$
<input type="checkbox"/> <b>EXCESS/UMBRELLA LIABILITY</b> <input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS MADE DEDUCTIBLE \$ RETENTION \$				EACH OCCURRENCE \$ AGGREGATE \$ \$ \$
<b>B</b> <b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (If yes, describe under SPECIAL PROVISIONS below) OTHER	SIR \$2,000,000	05/01/08	05/01/09	<input checked="" type="checkbox"/> WC STAT- TORY LIMITS <input type="checkbox"/> OTHER EL EACH ACCIDENT \$2,000,000 EL DISEASE - EA EMPLOYEE \$2,000,000 EL DISEASE - POLICY LIMIT \$2,000,000

### DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES / EXCLUSIONS ADDED BY ENDORSEMENT / SPECIAL PROVISIONS

RE: Memorandum of Agreement between USC and the City of Los Angeles Security Officers Agreement, as well as the liability assumed under the MOA between the insured and the Chief of Police of Los Angeles to the provisions of section 803.7 (b) PC.

\*Please see attached Notepad and form #GLX008I for further description

### CERTIFICATE HOLDER

CITYLAP  
City of Los Angeles, City of  
Los Angeles Police Dept./Board  
of Police Commissioners  
150 N. Los Angeles St, Rm. 150  
Los Angeles, CA 90012

### CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, THE ISSUING INSURER WILL ENDEAVOR TO MAIL 30\* DAYS WRITTEN NOTICE TO THE CERTIFICATE HOLDER NAMED TO THE LEFT, BUT FAILURE TO DO SO SHALL IMPOSE NO OBLIGATION OR LIABILITY OF ANY KIND UPON THE INSURER, ITS AGENTS OR REPRESENTATIVES.

UNIVERSITY OF SOUTHERN CALIFORNIA  
[Signature]

## IMPORTANT

If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must be endorsed. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

If **SUBROGATION IS WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

## DISCLAIMER

The Certificate of Insurance on the reverse side of this form does not constitute a contract between the issuing insurer(s), authorized representative or producer, and the certificate holder, nor does it affirmatively or negatively amend, extend or alter the coverage afforded by the policies listed thereon.

**NOTEPAD:**HOLDER CODE  
INSURED'S NAMECITYLAP  
University of So. CaliforniaUNIVE-5  
OP ID G2PAGE 3  
DATE 08/01/08

The City of Los Angeles, the Police Department, the Board of Police Commissioners, and all City Officers, Employees and Agents are additional insured per attached form #GLX008I as required by contract and to the extent insurable as their interests may appear with respect to the memorandum of agreement between USC and the City of Los Angeles Security Officers Agreement

\*10 day notice of cancellation for nonpayment of premium.  
All policy terms, conditions, limitations, and exclusions apply.



University of Southern California  
GLX20090015100

Effective: 8/01/2008

### ADDITIONAL INSURED

In consideration of the premium charged, we agree with the Educational Organization that, subject always to all other provisions of this Policy,

**The City of Los Angeles, the City of Los Angeles Police Department, and the Board of Policy Commissioners, and all City Officers, Employees, and Agents**

is an additional Insured but only with respect to Occurrences arising out of operations and functions for or on behalf of an Included Entity.

All other Policy provisions remain the same.

GLX0081

7/1/2004

United Educators Insurance, a Reciprocal Risk Retention Group



## Mission Special Enforcement Section Vehicle Check out Log

Date	Unit	Officer	Vehicle	Time out	Supv	Time In	Supv	Mileage Out	Mileage In
9-17-11				1700	(P)	0230	(P)	64984	65525
9-17-11			19649	1700	(P)	0230	(P)	39890	39976
9-17-11			CAMRY	1700	(P)	0230	(P)	76138	76132
9-19-11			19649	1300	WA	2130	WA	39976	40004
9-19-11			MAZDA	315	WA	2130	WA	23242	23307
9-19-11			GRY PONT	1500	WA	2130	WA	91569	91579
9-19-11			85062	1520	WA	2030	WA	76549	76602
9-21-11			GRY PONT	1500	WA	1930	WA	91579	91594
9-21-11			19621	1600	WA	1930	WA	23307	23324
9-21-11			86738	1700	WA	0100	(P)	76270	76340
9-22-11			19621	1600	(P)	0100	(M)	23324	23396
9-23-11			88681	1730	(P)	0300	(P)	35703	35772
9/24/11	FSC		89145	1800	FW	2200	FW	15890	15880
9-24			88681	1730	(P)	0230	(P)	25713	25860
9/27			19621	1230	WA	0010	WA	23465	23396
9/27/11			GRY PONT	1230	WA	2150	WA	91594	91601
9/28/11			19621	1300	WA	2100	WA	23465	23484
9/28/11			GRY PONT	1300	WA	2100	WA	91601	91681
9-28			85227	1630	(P)	0145	(P)	63470	63517
9-28			85227	1630	(P)				
9-29-11			GRY PONT	1245	WA	2100	WA	91681	91687
9-29-11			MAZDA	1245	2	2115	WA	23484	23531
9-29			86217	1715	(P)	0030	(P)	63525	63558
9-29			88681	1715	(P)	0030	(P)	36002	36043
9/29	FSC		89145	1200	FW	2140	FW	15960	15990
9/30			19621	1045				23531	
9/30			85227	1235				91687	

B/O 'C  
RTN TC  
MISS 9/2

# Mission Special Enforcement Section Vehicle Check out Log

Date	Unit	Officer	Vehicle	Time out	Supv	Time In	Supv	Mileage Out	Mileage In
9-1	F22	[REDACTED]	89145	1640	WA	0030		15654	15700
9-1-11	[REDACTED]	[REDACTED]	85941	1700	WA	2100	WA	106601	106604
9-2-11	[REDACTED]	[REDACTED]	86382	1230	FR	2000	FR	65208	65289
9/2/11	[REDACTED]	[REDACTED]	19621	1215	FR	2110	FR	22689	22710
9/2/11	[REDACTED]	[REDACTED]	19649	1305	FR	2000	FR	39486	39535
9/3/11	[REDACTED]	[REDACTED]	19621	1230	WA		WA	22710	22725
9/3/11	[REDACTED]	[REDACTED]	19649	1230	WA	1730	WA	39535	39541
9/6/11	[REDACTED]	[REDACTED]	19621	1230		2130		22425	22803
9/6/11	F22	[REDACTED]	89145	1720	WA	0200	WA	15700	15740
9/6/11	[REDACTED]	[REDACTED]	86382	1720	WA	0150	WA	65,299	65,321
9/6/11	[REDACTED]	[REDACTED]	19649	1345	WA	0330	WA	39541	39630
9/7/11	[REDACTED]	[REDACTED]	19621	1215	WA	1900	WA	22803	22850
9/7/11	[REDACTED]	[REDACTED]	19641	1100	WA	1900	WA	39636	39680
9/7/11	[REDACTED]	[REDACTED]	86382	1330	WA	2540	WA	65289	65406
9/7/11	F22	[REDACTED]	89145	1500	WA	2100	WA	15700	15781
9-7-11	[REDACTED]	[REDACTED]	TAXI	1400	WA	1930	WA	76485	76503
9-8-11	F24	[REDACTED]	89145	1610	WA	0130	WA	15,782	15,840
9-8-11	[REDACTED]	[REDACTED]	19621	1610	WA	0000	WA	22850	22915
9-11-11	[REDACTED]	[REDACTED]	19649	1200	WA	2100	WA	39680	39765
9-11-11	[REDACTED]	[REDACTED]	19621	1325	WA	2100	WA	22919	22970
9-11	[REDACTED]	[REDACTED]	CAMP4	1610	WA	0130	WA	78291	78850
9/12/11	[REDACTED]	[REDACTED]	19649	1210	WA	2130	WA	39765	39796
9-12	[REDACTED]	[REDACTED]	TAXI	1210	WA	1900	WA	76503	76549
9/12	[REDACTED]	[REDACTED]	19621	1300	WA	2100	WA	22970	23036
9-12-11	[REDACTED]	[REDACTED]	86738	1630	WA	0135	WA	78850	76029
9/13/11	[REDACTED]	[REDACTED]	19621	1445	WA	2130	WA	23036	23107
9/13/11	[REDACTED]	[REDACTED]	85227	1500	WA	2100	WA	91553	91568
9/13/11	[REDACTED]	[REDACTED]	19649	1200	WA	2100	WA	39796	39823
9/14/11	[REDACTED]	[REDACTED]	19621	1300	WA	2130	WA	23107	23170
9/14/11	[REDACTED]	[REDACTED]	19649	1230	WA	2200	WA	39823	39888
9/14/11	[REDACTED]	[REDACTED]	86382	1500	WA	0100		65406	65485
9/15/11	[REDACTED]	[REDACTED]	19649	1640		2100		39888	39890
9-15-11	[REDACTED]	[REDACTED]	19621	1300		2045		23179	23193
9-16-11	[REDACTED]	[REDACTED]	19621	1700	WA	0200	WA	23183	23241

- B10

RTN FROM  
GVB LOAN

MM

## Mission Special Enforcement Section Vehicle Check out Log

Date	Unit	Officer	Vehicle	Time out	Supv	Time In	Supv	Mileage Out	Mileage In
8/8/11			19639	1215	FL	2300	FL	56736	56745
8/9/11			19645	1230	FL	2130	FL	39170	39172
8/9/11			19639	1245	FL	2140	FL	56745	56756
8/9/11			86382	1600	FL	0130	FL	64656	64695
8/16/11			19639	0600	WA	1600	WA	56756	56816
8/17/11			19621	1125	WA	1900	WA	22462	22538
8/17/11	F26		89145	1420	WA	0000	FL	15437	15458
8/17/11			86382	1720	WA	2355	FL	64174	64826
8-17-11			14649	0900	WA	1900	WA	39142	39233
8-18-11			86382	0530	WA	1400	FL	64827	64856
8-18-11	F26		89145	1610	FL	0100	WA	15458	15487
8-18-11			86382	1730	FL	0000	WA	64826	64875
8-19-11	F22		89145	1700	WA	0330	WA	15487	15597
8-19-11			86382	1700	WA	0330	WA	64875	64985
8-20-11			86382	1200	WA	0300		64985	65055
8-24-11			AVALON	1135	WA	-	-	56816	RTN To the name FOX
8/24/11			FORD	1300	WA			39233	39262
8/24/11			MAZDA	1400	WA	2030		22539	22562
8/25/11			MAZDA	1245	WA	2115	WA	22562	22591
8/25/11			FORD	1245	WA	2200	WA	39262	39320
8/25/11			86382	1620	WA	0700	RTN	65055	65114
8/25/11			85941	1815	WA	2115	WA	106531	106580
8/26/11			FORD	1720	WA	2100	WA	39320	39378
8/26/11			MAZDA	1300		2100	WA	22591	22612
8/26/11			85941	1400	WA	2045	WA	106580	106590
8/31/11			MAZDA	1245	WA	2145	WA	22612	22672
8/31/11			FORD	1245	WA	2150	WA	39378	39408
8-31-11			86382	1245	WA	2130	WA	65114	65150
8-31-11			TAXI	1400	WA	1430	WA	76482	76485
8-31-11			85941	1430	WA	2130	WA	106590	106601
8-31-11	F22		89145	1730	WA	0130	WA	15597	15654
9-1-11			86382	1230	WA	2155	FL	65150	65208
9/1/11			FORD	1730	WA	2130	WA	39408	39486
9/1/11			MAZDA	1300	WA	2130	WA	22672	22689

# Mission Special Enforcement Section Vehicle Check out Log

Date	Unit	Officer	Vehicle	Time out	Supv	Time In	Supv	Mileage Out	Mileage In
7-19-11			86382 HYBRID	1600	PKY	0000	PKY	-	-
7-19-11	F26		89145	1600	PKY	0000	PKY	-	-
7-19-11			86382 MAZDA	1200	PKY		PKY	22265	22284
7-20-11			MAZDA	1200	PKY	2100	PKY	22284	22335
7-20-11	F38		89145	0600	PKY	1700	PKY	14461	14517
7-20-11			19639	2015	PKY	2100	PKY	56281	56285
7-21-11			MAZDA	1230	PKY	2100	PKY	22335	22412
7-21-11	F38		89145	1430	PKY	0130	PKY	14577	14650
7-21-11			19639	1445	PKY	2200	PKY	56285	56301
7-21-11			19639	1215	PKY	2200	PKY	56301	56390
7-21-11	F38		89145	1400	PKY	0000	PKY	14665	14715
7-21-11			19639	1245	PKY	2115	PKY	56390	56487
7-21			HYBRID	1400	PKY	0200	PKY	64300	64340
7-22			ESCAPE	1200	PKY	2100	PKY	38730	38770
7-23-11			ESCAPE	1200	PKY	2100	PKY	38770	38824
7-23-11			19639	1600	PKY	2100	PKY	56487	56501
7-24-11			19639	1630	PKY	2200	PKY	56501	56554
7-30-11			HYBRID	1700	PKY	0300	PKY	64340	64380
8-1-11	F38		89145	1700	PKY	0300	PKY	14865	14935
7-30-11			86382	1730	PKY	0300	PKY	64380	64430
7-31-11			19639	1300	PKY	1515	PKY	56554	56578
7-31-11			19649	1300	PKY	1300	PKY	B	0
7-31-11			MAZDA	1300	PKY	1515	PKY	24222	24446
7-31-11			CAMRY	1300	PKY	1515	PKY	74785	74812
8-2-11	F38		89145	1700	PKY	2200	PKY	14955	15026
8-2-11			19649	1600	PKY	2100	PKY	38827	38894
8-3-11			19639	1230	PKY	2100	PKY	56578	56795
8-4-11			19639	1515	PKY	2140	PKY	38894	38836
8-4-11	F38		89145	1600	PKY	0500	PKY	15027	15076
8-4-11			FORD	1200	PKY	2000	PKY	38894	38957
8-6-11			MAZDA	2200	PKY	2330	PKY	24222	24262
8-6-11	F22		LPR	1700	PKY	0500	PKY	15076	15108
8-6-11			HYBRID	1700	PKY	0300	PKY	64508	64558
8-8-11			FORD	1200	PKY	2500	PKY	38957	39101

# Mission Special Enforcement Section Vehicle Check out Log

Date	Unit	Officer	Vehicle	Time out	Supv	Time In	Supv	Mileage Out	Mileage In
6-29-11			X-TERRA	1300	WA	1900	WA	64500	64516
6/29/11			MAZDA	1700	WA	2200	WA	<del>22045</del>	22045
6/30/11			MAZDA	1200	WA	2200		22045	22085
6/30/11			X-TERRA	1230	WA	1730	WA	64566	64581
6/30/11			LPR	1400					
6/30/11			AVALON	1530	WA	2000	WA	56099	56131
6/30/11			89145	1650	WA	0115	FS	13616	13680
6/30/11			TAXI	1640	WA	2000	WA	76460	76476
7/1/11			88388	1715	WA	0300	WA	23853	23910
7/2/11			88388	1730	WA	0230	WA	23926	23972
7/6/11	F32		89145	0700	AL	1600	AL	13812	13887
7/6/11			X-TERRA	1100	WA	1400	WA	64581	64585
7/6/11			AVALON	1730	WA	2040	WA	56131	56155
7/7/11			X-TERRA	1330	WA	2120	WA	64585	64626
7/7/11	F32		89145	0700	WA	1700	WA	13888	13998
7/7/11	F28		89145	1700	WA	0600	WA	13998	
7/7/11			AVALON	1700	WA	2120	WA	56155	56172
7/7/11			MAZDA	1700	WA	2120	WA	22085	22125
7/8/11			X-TERRA	1230	WA	2115	WA	64626	64676
7/8/11			MAZDA	1430	WA	2115	WA	22125	22165
7/8/11			AVALON	1500	WA	2115	WA	56172	56175
7/8/11	F28		89145	1700	WA	1630	WA	14085	14145
7/12/11			89145	1200	WA	1230	WA	14145	14210
7/12/11			X-TERRA	1200	WA	1845	WA	<del>56232</del>	56232
7/12/11			AVALON	1330	WA	2130	WA	56175	56218
7/13/11			X-TERRA	1230	WA	1600	WA	56232	
7/13/11			89145	1650	WA			14210	
7/13/11	F34		89145	1230	WA	2145	WA	14210	14260
7/13/11			MAZDA	1230	WA	2100	WA	22165	22187
7/14/11	F34		89145	1230	WA	2130	WA	14260	14320
7/14/11			AVALON	1300	WA	2100	WA	56218	56239
7/14/11			MAZDA	1410	WA	1900	WA	22140	22187
7/14/11			AVALON	1310		1900		56239	56241

B/O A/C AT DEPT 3

BACK TO DEPT 3







75	241	D	License Plate Recognition Program	Computer servers and server components which includes warranty and service to support the ALPR system.	Los Angeles Police	14.1.1.7	Systems, Video Assessment	5	1034832	Dell		152,316	18	Sep-09	G3Q8GD1	New	ITB: 100 W 1st St Room 842, Los Angeles, CA
75	241	D	License Plate Recognition Program	Computer server storage and components which includes warranty and service to support the ALPR system.	Los Angeles Police	14.1.1.7	Systems, Video Assessment	3	1034832	Dell		51,975	18	Sep-09	UASI-06-2-211-001, UASI-06-2-212-001, UASI-06-2-212-002	New	ITB: 100 W 1st St Room 842, Los Angeles, CA
75	241	D	License Plate Recognition Program	Computers which includes warranty and service to support the ALPR system.	Los Angeles Police	14.1.1.7	Systems, Video Assessment	10	1034832	Dell		25,695	18	Sep-09	UASI-06-2-213-001 through 010	New	ITB: 100 W 1st St Room 842, Los Angeles, CA
75	241	D	License Plate Recognition Program	Double take and network diskbackup software for the computer servers to support the ALPR system.	Los Angeles Police	14.1.1.7	Systems, Video Assessment	2	1040917	CompuCom		39,850	18	Sep-09	n/a	New	ITB: 100 W 1st St Room 842, Los Angeles, CA
75	241	D	License Plate Recognition Program	Train the trainer training to be provided by the vendor to LAPD personnel on the installation and usage of the ALPR equipment. As a result of the train the trainer training, the installation and usage of the ALPR equipment will be done in house by LAPD. The total cost of the training will include travel costs to attend the train the trainer course provided by the vendor.	Los Angeles Police	21.8	Consulting Services in Support of Equipment Acquisition.	1		PIPS		7,323	31	3/15/2010 - 3/18/2010	n/a	n/a	Trng @ PIPS HQ for Software configuration & installation. Knoxville, TENNESSEE
75	241	D	License Plate Recognition Program	Train the trainer training to be provided by the vendor to LAPD personnel on the installation and usage of the ALPR equipment. As a result of the train the trainer training, the installation and usage of the ALPR equipment will be done in house by LAPD. The total cost of the training will include travel costs to attend the train the trainer course provided by the vendor.	Los Angeles Police	21.8	Consulting Services in Support of Equipment Acquisition.	1				1,146					

# **Exhibit D**

**INTRADEPARTMENTAL CORRESPONDENCE**

March 1, 2013  
1.17

**TO:** The Honorable Board of Police Commissioners

**FROM:** Chief of Police

**SUBJECT:** TRANSMITTAL OF THE EXTENSION FOR THE 2009 LOS ANGELES SMART POLICING PROJECT

**RECOMMENDED ACTIONS**

1. That the Board of Police Commissioners (the Board) REVIEW and APPROVE this report.
2. That the Board TRANSMIT the report concurrently to the Mayor and City Council.
3. That the Board REQUEST the Mayor and City Council to:
  - A. AUTHORIZE the Chief of Police or his designee to ACCEPT the 2009 Los Angeles Smart Policing Project no-cost extension from the United States Department of Justice, Office of Justice Programs, Bureau of Justice Assistance (BJA) for a new grant term of October 1, 2009 through June 30, 2013;
  - B. AUTHORIZE the Chief of Police or his designee to execute the Fourth Amendment to Contract No. C-118498 with Justice and Security Strategies, Inc., to extend the term of the contract by four months from February 28, 2013 to June 30, 2013, for a new contract term of May 1, 2010 through June 30, 2013, subject to approval of the City Attorney as to form and legality;
  - C. AUTHORIZE the Controller to transfer appropriations within Fund No. 339, Department No. 70 from the 2009 Los Angeles Smart Policing Appropriation Account Number 70F550 to the following accounts:

Account No.

<u>Account No.</u>		<u>Amount</u>
70J170	Civilian Salaries	\$19,505.00
70J299	Fringe Benefits	\$ 7,216.45

- D. AUTHORIZE the Los Angeles Police Department (LAPD) to prepare Controller Instructions for any necessary technical adjustments, subject to the approval of the City Administrative Officer, and AUTHORIZE and INSTRUCT the Controller to implement the instructions.

## DISCUSSION

The LAPD is seeking approval to accept a four-month, no-cost extension for the Los Angeles Smart Policing Project from BJA. The focus of this grant has been to reduce gun violence in Newton Area and to support the use of predictive analytics and other technology that would assist officers in targeting chronic locations and chronic offenders. Newton Area has been successful in reducing violent crime (homicides, robberies, and gun-related crime) through Operation LASER (Los Angeles' Strategic Extraction and Restoration program). A BJA Spotlight was published and is currently on the Smart Policing website. Newton Area continues to implement Operation LASER and Dr. Uchida of Justice & Security Strategies, Inc., continues to evaluate its effects. An extension would allow Dr. Uchida to analyze data through the first quarter of 2013. This would mean a 20-month period to measure the intervention and perhaps show the sustainability of Operation LASER in one Area.

In addition, the extension will allow crime analysts, officers, and detectives to be trained on Palantir, a platform that allows for the use of multiple databases in one place. Recently, we received preliminary approval, pending a Grant Adjustment Notice submission, for the expansion of a training room at Real-Time Analysis and Critical Response Division for the purpose of increasing the number of students who could be trained on the technology. Palantir has been used by Newton Area's Crime Intelligence Detail to create Chronic Offender Bulletins, to track vehicles using data from the Automated License Plate Reader, to examine social networks, and for other investigative purposes. The expansion of the training room is not yet completed and will require additional time for the new workstations to be wired and finished.

If you have any questions regarding this matter, please contact Chief Information Officer Maggie Goodrich, Commanding Officer, Information Technology Bureau, at (213) 486-0370.

Respectfully,



CHARLIE BECK  
Chief of Police

Attachments

**INTRADEPARTMENTAL CORRESPONDENCE**

February 20, 2013  
1.17

**TO:** Chief of Police

**FROM:** Commanding Officer, Information Technology Bureau

**SUBJECT:** TRANSMITTAL OF THE EXTENSION FOR THE 2009 LOS ANGELES  
SMART POLICING PROJECT

Attached for your approval and signature is an Intradepartmental Correspondence to the Board of Police Commissioners requesting approval for the no-cost extension for the 2009 Los Angeles Smart Policing Project, from the United States Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, extending the award period from February 28, 2013 to June 30, 2013.

The focus of this grant has been to reduce gun violence in Newton Division and to support the use of predictive analytics and other technology that would assist officers in targeting chronic locations and chronic offenders. Newton Division has been successful in reducing violent crime (homicides, robberies, and gun-related crime) through Operation LASER (Los Angeles' Strategic Extraction and Restoration program). An extension would allow Dr. Uchida to analyze data through the first quarter of 2013. This would mean a 20-month period to measure the intervention and perhaps show the sustainability of Operation LASER in one division.

In addition, the extension will allow crime analysts, officers, and detectives to be trained on Palantir, a platform that allows for the use of multiple databases in one place. Palantir has been used by Newton Division's Crime Intelligence Detail to create Chronic Offender Bulletins, to track vehicles using data from the Automated License Plate Reader, to examine social networks, and for other investigative purposes.

If you have any questions, Senior Management Analyst Stella Larracas, Officer in Charge, Grants Section, is available to assist you at (213) 486-0393.



MAGGIE GOODRICH, Chief Information Officer  
Commanding Officer  
Information Technology Bureau

Attachment



US DEPARTMENT OF JUSTICE  
OFFICE OF JUSTICE PROGRAMS



### GRANT ADJUSTMENT NOTICE

[All Active](#)  
[Change Requested](#)

[Approved](#)

[Denied](#)

[Draft](#)

[Create Grant Adjustment](#)

[Help/Frequently Asked Questions](#)

Grantee Information				
<b>Grantee Name:</b>	City of Los Angeles	<b>Project Period:</b>	10/01/2009 - 06/30/2013	<b>GAN Number:</b> 017
<b>Grantee Address:</b>	200 N. SPRING ST SW MEZZANINE RM M175 LOS ANGELES, 90012	<b>Program Office:</b>	BJA	<b>Date:</b> 01/30/20
<b>Grantee DUNS Number:</b>	03-784-8012	<b>Grant Manager:</b>	Melanie Davis	
<b>Grantee EIN:</b>	95-6000735	<b>Application Number(s):</b>	2009-H2154-CA-D2	
<b>Vendor #:</b>	956000735	<b>Award Number:</b>	2009-DG-BX-0118	
<b>Project Title:</b>	Los Angeles Smart Policing Project	<b>Award Amount:</b>	\$499,959.00	

Change Project Period				
<b>Current Grant Period:</b>	Month: 40 Day: 27	<b>New Grant Period:</b>	Month: 44 Day: 29	
<b>Project Start Date:</b>	10/01/2009	<b>*New Project Start Date:</b>	10/01/2009	
<b>Project End Date:</b>	02/28/2013	<b>*New Project End Date:</b>	06/30/2013	

**\* Required Justification for Change Project Period:**

The Los Angeles Police Department (LAPD) requests a 4-month no-cost extension to complete the evaluation of Operation LASER in Newton Division and allow training of personnel on Palantir. Most recent unobligated balance is \$102,368.55. See attachment.

**Attachments:**

Filename:	User:	Timestamp:	Action:
No cost extension 012413.docx	LAPDGRANTS	01/25/2013 3:00 PM	<a href="#">Delete Attachment</a>

**Actions:**

[Close](#)

[Printer Friendly Version](#)

**Audit Trail:**

Description:	Role:	User:	Timestamp:	Note:
Approved-Final	OCFMD - Financial Analyst	SYSTEM_USER	01/30/2013 12:01 PM	<a href="#">View Note</a>
Submitted	PO - Grant Manager	LAPDGRANTS	01/25/2013 3:01 PM	<a href="#">View Note</a>
Change Requested	EXTERNAL - External User	davism1	01/25/2013 9:43 AM	<a href="#">View Note</a>
Change Requested	PO - Grant Manager	davism1	01/25/2013 9:43 AM	<a href="#">View Note</a>
Submitted	PO - Grant Manager	LAPDGRANTS	01/24/2013 8:21 PM	<a href="#">View Note</a>
Draft	EXTERNAL - External User	LAPDGRANTS	01/24/2013 8:20 PM	<a href="#">View Note</a>
Draft	EXTERNAL - External User	LAPDGRANTS	01/24/2013 8:16 PM	<a href="#">View Note</a>

1 **PROOF OF SERVICE**

2 STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

3 I am employed in the County of Los Angeles, State of California. I am over the age of 18  
4 and not a party to the within action. My business address is 1313 West Eighth Street, Los  
5 Angeles, California 90017. I am employed in the office of a member of the bar of this court at  
6 whose direction the service was made.

7 On January 24, 2014, I served the foregoing document: DECLARATION OF PETER  
8 BIBRING IN SUPPORT OF MEMORANDUM OF POINTS AND AUTHORITIES IN  
9 SUPPORT OF PETITION FOR WRIT OF MANDAMUS, EXHIBITS A-D on the parties in  
10 this action by placing a true and correct copy of each document thereof, enclosed in a sealed  
11 envelope, addressed as follows:

12 Tomas A. Guterres  
13 Eric C. Brown  
14 Collins Collins Muir & Stewart LLP  
1100 El Centro Street  
South Pasadena, CA 91030

15 Heather L. Aubry, Deputy City Attorney  
16 City Hall  
200 North Main Street  
17 City Hall East, Room 800  
Los Angeles, CA 90012

18 I caused such envelope(s) fully prepaid with U.S. Postage to be placed in the United  
19 States Mail at Los Angeles, California. I am "readily familiar" with the firm's practice of  
20 collection and processing correspondence for mailing. Under that practice it would be deposited  
21 with the U.S. Postal Service on that same day with postage thereon fully prepaid at Los Angeles,  
22 California in the ordinary course of business.

23 I declare under penalty of perjury under the laws of the State of California and the United  
24 States of America that the above is true and correct.

25 Executed on January 24, 2014, at Los Angeles, California.

26  
27   
28 Geneva Tien