City of San Leandro

Meeting Date: September 3, 2013

Staff Report

File Number: 13-430 **Agenda Section:** ACTION ITEMS

Agenda Number: 10.B.

TO: City Council

FROM: Chris Zapata
City Manager

BY: Sandra Spagnoli
Chief of Police

FINANCE REVIEW: Not Applicable

TITLE: Staff Report for Public Safety Camera Planning and Policy Considerations

SUMMARY AND RECOMMENDATIONS

Staff is currently replacing all security cameras in City Hall and the Police Department due to the age and poor quality of the equipment. As part of this project, staff is formulating plans to add (in two locations) public safety cameras, focused on discrete public places that include Automatic License Plate Readers (ALPRs). Staff recommendations meet the guidelines published by the United States Department of Justice Community Oriented Policing Services office and research conducted by The Urban Institute Justice Policy Center.

Staff recommends the following actions:

1. Discussion of a proposed policy related to the City's use of public safety cameras. A draft policy will be brought back to the City Council for consideration and approval.
2. Authorization to bring a project to the City Council to consider replacement of the public safety cameras at City Hall and the Police Department. The project would include public safety cameras with license plate readers at two public locations, expanding the City's existing ALPR program.

DISCUSSION

The Police Department presented its annual report to the City Council at the end of 2012. During that presentation, staff reported that it would review the use of public safety cameras to enhance the current law enforcement and crime deterrent technology in use by the City. Staff work has progressed such that staff believes that the City Council should consider a public safety camera policy prior to the enhanced use of public safety cameras. The inclusion of automated license plate readers as part of this project is covered by an existing policy. The Police Department currently has one automated license plate reader in use in a patrol vehicle and two parking automated license plate readers in the parking aide vehicles.

The Police Department currently has limited use of video monitoring in the below areas:

1. Police Department (Internal, including the jail)
2. Police Department (External, including parking areas)

The effective use of public safety cameras can increase a police department's ability to control, reduce and prevent crime. Local municipalities already have or are considering strategic placement of public safety cameras to enhance current public safety and crime prevention programs and deter illegal activities. Public safety cameras provide for greater coverage of a geographical area than police department personnel can provide. Public safety cameras can also be used as a force multiplier, enhancing a Police Department's ability to better utilize its staffing resources. For example, public safety cameras provide for:

1. **Strong evidence to support prosecution.** Public safety camera views can provide visual evidence of crimes in progress and/or the evidence left behind leading to prosecutable arrests.

2. **Enhanced crime prevention.** Public safety cameras are effective as a crime prevention strategy through deterrence of criminal acts. Several examples are listed below:

    a. **City of Pittsburg, CA** installed 5 cameras in 2005 and increased to a total of 86 cameras in 2013. From 2004 to 2011, they experienced a 22.5% reduction in part I crime. To date, they have a 20% decrease in Part 1 crime compared to 2004. Since 2005, overall violent crime has declined 46.7%. Pittsburg credits the cameras to being a major factor in crime reduction, along with Redevelopment, increased community partnerships, and effective officer-deployment strategies.
    b. **City of Fairfield**, **CA** has had cameras for 5 years and currently has 100 cameras. Video from these cameras has been used to solve homicides and also a recent high profile kidnapping/ murder case.
    c. **City of Martinez**, **CA** has 12 cameras and reports a reduction in crime in areas with cameras.
    d. **City of Richmond, CA** has over 70 cameras which have assisted in solving street crimes.
    e. **City of Fresno, CA** has over 150 cameras and has been credited to solving major crimes. The program has been in place since 2006. The cameras have captured a shooting and have deterred crime.
    f. **City of Ripon, CA** installed over 70 cameras and captured dozens of crimes and has assisted in capturing suspects and solving crime.
    g. **Alameda County, CA** installed cameras in seven locations. The cameras have been of great assistance, providing direct evidence and leads in solving crime. In the last year, the cameras have helped solve many crimes including a felony assault on an officer.

Both Fairfield and Richmond allow the public to fund a portion or all of a camera for a location approved by the police department.

3. **Better protection for citizens in the community.** Police personnel are more effective in identifying suspects or suspicious circumstances for further investigation and possible enforcement activity. Public safety cameras can help ensure that state laws and local ordinances are consistently enforced through better enforcement.

How will the City determine the effectiveness of the public safety camera program?

The San Leandro Police Department will set program goals and use data to measure such results against stated goals for the program to determine if the use of public safety cameras is effective. For example, the Police Department could measure response times to crimes recently committed and crimes in progress; successful prosecutions that occurred with the aid of evidence obtained through public safety cameras; and arrest analytics that will include but not be limited to types of crimes, and locations of where those crimes were committed. From this data, the Police Department believes it can generate an evaluation of the overall public safety benefits.

What social considerations should be considered?

Concerns regarding the use of public safety cameras usually involve potential violations of civil liberties and individual privacy rights. The City is sensitive to such concerns, and will work to create a policy that mitigates the risk that such violations occur. The City will work to educate the public on the use policies for public safety cameras. The policy will address Fourth Amendment rights protecting citizens from unreasonable search and seizure by, for example, providing that cameras should only be used where there is no constitutionally protected expectation of privacy. Consideration will be given towards notifications indicating that public safety cameras are in use and/or recording. However, the policy must balance such considerations against covert use by the Police Department of such cameras where it may be both beneficial and appropriate in certain circumstances where apprehending suspects during the commission of certain crimes is the desired goal. Finally, the appropriate training of law enforcement officers can prevent unlawful recordings and the use of recordings for purposes other than those originally intended.

The Police Department, along with the City Attorney's Office, will research the legal considerations of implementing public safety cameras for solving and preventing crime.

Some frequently asked questions and responses related to public safety cameras are listed below:

1. Is it legal for police to videotape citizens without their consent or knowledge?

Yes. As long as the cameras are recording public places, there are no violations of a citizen's reasonable expectation of privacy. Policies and protocols, and proper training and supervision will be in place to reduce risks of misuse.

2. What, if any, are the constitutional limits on the use of cameras in public places?

The "reasonable expectation of privacy" is essentially part of the Fourth Amendment right for persons to be free from unreasonable searches and seizures. Restricting monitoring to public

places, which by law and custom cause persons to have diminished expectations of privacy is the main legal restriction.

3. What would be an example of a place the cameras could not monitor?

All efforts will be made to place cameras in such a way that the interior of any residence, backyard or other private structure are not in viewing range.

4. What are some examples of places where the cameras could monitor?

Sidewalks, streets, intersections, parks, public buildings, beaches, trails, vehicles (interior and exterior), parking lots, walkways and all other public areas.

5. Are there other places that use cameras/ public cameras?

Public agencies nationwide use public safety cameras. Private businesses use private security cameras for many purposes, especially loss prevention, extensively throughout California. Public safety camera systems are used on city streets, sidewalks and city parks in both residential and commercial neighborhoods. Cities like Chicago, New Orleans, and Minneapolis have extensive law enforcement camera operations. Closer to home, the cities of Stockton, Clovis, Gilroy, Alameda County, San Francisco, Pittsburg, Brentwood, Concord, and Pinole use public safety cameras to varying degrees. Piedmont and Oakland are currently developing public safety camera programs.

6. Is any action required to implement cameras?

No. The public safety camera system may legally be installed and implemented through the existing City purchasing policies.

7. Are there any legal requirements regarding posting of notices that cameras are in use?

No, there is no legally mandated notice requirement. The cameras may be used in an "undercover" capacity to monitor any public place. The same placement restriction (only places open to the public) applies to the use of both marked and unmarked public safety cameras.

8. Are recordings public records?

Yes, recordings would be considered public records under the California Public Records Act. The disclosure of such records upon request would be subject to the applicable exemptions codified in the Public Records Act.

9. What is the retention requirement for public safety camera data that is recorded?

The California Government Code mandates a minimum one-year retention period for such recordings (California Government Code section 34090.6). However, this period may be reduced if the City complies with California Government Code section 34090.7 and keeps, for

example, a duplicate record such as written minutes of specific time recorded.

Operational Considerations:

A public safety camera project should cover:

1. Camera type and features
2. System infrastructure
3. Camera locations and staff recommendations
4. Criteria used for camera location

What are some recommended policies and procedures?

The Security Industry Association and the International Association of Police have established guidelines for law enforcement in the use of public safety cameras in public areas. The guidelines recommend:

1. Information obtained from public safety cameras should be used exclusively for safety and law enforcement purposes.
2. Information obtained through the use of public safety cameras should be handled according to the accepted law enforcement procedures and legal rules governing the handling of evidence, protecting anonymity and personal privacy, and also private property.
3. Establishment of an on-going program assessment.
4. Dissemination of information should be conducted in accordance with applicable state and federal laws.
5. Unusable or non-case specific data should not be retained and thus purged within a legally appropriate time, ensuring evidence quality and integrity.
6. All local law enforcement agency personnel involved with public safety cameras should receive appropriate training applicable to criminal and civil law.
7. Unauthorized use of the public safety cameras system will result in disciplinary action.

How can the City assure the community that policies and procedures are followed?

The Police Chief would review complaints regarding camera locations and usage and ensure that policies and procedures are being followed.

Other considerations for public safety cameras:

Part of the criteria for the placement of public safety cameras should be that they are placed in locations that are legal, tactically strategic to maximize the enhancement of crime prevention and enforcement, and not vulnerable to extreme elements, tamper-resistant and enclosed in protective cases.

Current Agency Policies:

Attached to this report is:

- Current SLPD policy on Automated License Plate Readers

- Draft policy on Public Safety Cameras

The proposed policy includes:

1. Purpose and Scope
2. General Principles
3. Procedures
4. Responsibilities
5. Training/ Oversight
6. Retention/ Extraction and Storage Procedure
7. Audits
8. Complaint process
9. Annual Review of the public safety camera system

Committee Review and Actions

Members of the Chief's Advisory Board held two meetings to discuss a draft policy, and general comments from the board are attached. The recommended policy includes comments and recommendations from these meetings. In an informal vote, the majority of the group supported this project, while several opposed moving a project forward.

Legal Analysis

The City Attorney's Office is advising the Police Chief and staff on the policy and its implementation, including this staff report. All information will be vetted by the City Attorney before public release.

Fiscal Impacts

The Information Technology Department is currently working with a consultant to manage the City Hall security camera replacement project, which is in the budget. There is no additional fiscal impact at this stage of the program's development. Future fiscal impacts are dependent on City Council approval of a project.

ATTACHMENTS

1. Current ALPR Policy
2. NCRIC (Northern California Regional Intelligence Center) Privacy Impact Assessment for ALPR Technology
3. Draft Public Camera Policy
4. Summary of feedback on camera discussion from Chiefs Advisory Board

PREPARED BY: Sandra Spagnoli, Police Chief, Police Department

2128358.1

Automated License Plate Readers (ALPRs)

462.1 PURPOSE AND SCOPE

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition, provides automated detection of license plates. ALPRs are used by the San Leandro Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

462.2 ADMINISTRATION OF ALPR DATA

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

462.3 ALPR OPERATION

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement purposes.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

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

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

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

(f) If practicable, the officer should verify an ALPR response through CLETS before taking enforcement action that is based solely on an ALPR alert.

462.4 ALPR DATA COLLECTION AND RETENTION

All data and images gathered by an ALPR are for official use only and because such data may contain confidential CLETS information, it is not open to public review. ALPR information gathered and retained by this department may be used and shared with prosecutors or others only as permitted by law.

The Support Services Manager is responsible to ensure proper collection and retention of ALPR data, and for transferring ALPR data stored in department vehicles to the department server on a regular basis, not to exceed 30 days between transfers.

All ALPR data downloaded to the server should be stored for one year, and thereafter may be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

462.5 ACCOUNTABILITY AND SAFEGUARDS

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

(a) All non-law enforcement requests for access to stored ALPR data shall be referred to the Support Services Manager and processed in accordance with applicable law.

(b) All ALPR data downloaded to the mobile workstation and server shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

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

(d) Such ALPR data may be released to other authorized and verified law enforcement officials and agencies at any time for legitimate law enforcement purposes.

(e) Requests to review stored data shall be documentented and maintained in the same manner as criminal history logs.

(f) All transmission and storage of ALPR data shall meet CLETS requirements for network and computer security.

(g) ALPR system audits should be conducted on a regular basis.

Northern California Regional Intelligence Center
Initial Privacy Impact Assessment for
Automated License Plate Reader Technology

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens of the fifteen Bay Area counties within its area of responsibility from the threat of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

Fundamental to carrying out the NCRIC's responsibilities is doing so in a way that effectively protects the privacy and civil liberties of individuals and the security and confidentiality of sensitive information. To that end, and although not required by law to do so, the NCRIC has developed this initial Privacy Impact Assessment (PIA) for use, analysis, dissemination, retention, and destruction of data derived from the operation of NCRIC Automated License Plate Readers (ALPR) and ALPR systems of our partner law enforcement entities (ALPR Data).

In addition, the NCRIC has initiated development of, and will continue to refine, specific policy and guidelines for the use, analysis, dissemination, retention, and destruction of ALPR Data at the NCRIC (NCRIC ALPR Policy). To the greatest extent feasible, the NCRIC ALPR Policy will be made publicly available for review and comment.

Scope of this Initial Privacy Impact Assessment

This Privacy Impact Assessment applies to ALPR Data collected by the NCRIC and NCRIC partner agencies and shared with other regional law enforcement agencies, accessed, and analyzed using software hosted by the NCRIC. It is not intended to apply, and does not apply, to any other types of data accessed or used at the NCRIC or to any collection, use, or handling of any data at individual NCRIC member or contributing entities.

Use and Efficacy of Automated License Plate Reader Data

Automated License Plate Reader Technology

ALPR systems function to automatically capture an image of a vehicle's license plate, transform that image into alphanumeric characters using optical character recognition software, and store that information along with relevant metadata (i.e., geo-location and temporal information, as well as data about the ALPR unit).

At the NCRIC, such ALPR Data is accessed and analyzed using customized software to enable:

- Searches of full plates, with full color pictures of identified vehicles for plate read verification;
- Partial plate searches that return possible matches to assist in identifying suspects' vehicles;
- Geo-spatial searches of ALPR Data to assist in identifying possible suspects' vehicles in cases where other vehicle identification information exists;
- Creation of alert mechanisms for identification of license plates associated with, for example, active criminal investigations, Amber Alerts, and/or other authorized law enforcement and public safety purposes; and
- Use of these search capabilities across ALPR Data from contributing NCRIC member entities within a single interface and subject to the use, analysis, retention, destruction, sharing, and disclosure restrictions of the NCRIC and of the entities contributing the ALPR Data.

Adoption and Efficacy of ALPR Technology

More than 70% of U.S. police agencies surveyed in 2012 indicated that they are using ALPR technology.[1] Police agencies around the country have reported notable successes using ALPR technology in identifying suspects in domestic kidnappings, solving homicide cases, support for bomb detection units, reducing auto theft, and stolen vehicle recovery.[2]

Privacy and Civil Liberties Implications of ALPR Data

To date, United States courts and federal and state legal authorities have not found a legitimate expectation of privacy for individuals in ALPR Data and, as of the date of this initial PIA, no federal or California statutes applicable to the NCRIC or its partner agencies regulate the use of such data. Nonetheless, the NCRIC recognizes that the benefits to public safety of the effective use of ALPR Data by law enforcement are tempered by the risks posed by inadvertent or intentional misuse of such data to

[1] *How Innovations in Technology are Transforming Policing*, Police Executive Research Forum, 2012, at 1 (http://policeforum.org/library/critical-issues-in-policing-series/Technology_web2.pdf)
[2] *Id.* at 28-32.

individual privacy and civil liberties, and, more broadly, to the fundamental freedoms that make our society strong.[3]

Potential Individual Privacy and Civil Liberties Harms

Identification of Individuals. Although ALPR Data, by itself, does not identify individuals by name or provide other personal information, a license plate number can be used to determine the registered owner, and information about that person from, for example, state motor vehicle data. However, images taken by ALPR cameras may at times inadvertently include more information than just a license plate number. If misused, such information could result in harm to individuals, including but not limited to: assumptions about an individual's behavior or associations, personal agendas of individuals accessing the data, or furthering government objectives that are legitimate but beyond the permissible scope for which access to such data was authorized.

Misidentification. Without careful, rigorous, and technically-controlled access and use of ALPR Data, significant risks of individuals being misidentified as criminal suspects can arise.

Data Quality and Accuracy Issues. Related to misidentification are the challenges of data quality and accuracy. If ALPR Data associated with individuals and information analyzed along with such data is not kept up to date and accurate, governmental action may be improperly taken against such individuals and unwarranted investigative assumptions may be made.

Non-relevant data. Data regarding a vehicle's location – particularly when collected over an extended period of time – could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities. By precisely and proportionally limiting access to ALPR Data, the risks of such misuse can be reduced and the likelihood of inferring protected/non-relevant character attributions can be minimized.

These, of course, are not the only potential individual privacy and civil liberties harms from misuse of ALPR Data. Such potential harms have been widely discussed in recent years, including in the 2009 ALPR Privacy Impact Assessment produced by the International Association of Chiefs of Police, and resources cited therein, and by the American Civil Liberties Union.[4]

---

[3] Such concerns have been reflected in recent judicial and legislative activities. *See, e.g., United States v. Jones* (quoted below); California Senate Bill 1330. A right to privacy is explicitly enshrined in Section 1 of the California Constitution.

[4] http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87 (This "Privacy impact assessment report for the utilization of license plate readers," published by the

Potential Societal Harms

Perhaps of even greater long-term concern than the risks to individual privacy and civil liberties harms discussed above, which are inherent in any governmental access, use, and storage of information about individuals, are the emerging risks to our societal values themselves. The American Civil Liberties Union has warned, for example, that as ALPR Data becomes more voluminous and analysis of that data more powerful, there is a risk to society that ALPR Data could cease "to be simply a mechanism enabling efficient police work and [become] a warrantless tracking tool, enabling retroactive surveillance of millions of people."[5]

In the landmark 2012 United States Supreme Court decision in *US v. Jones*, Justice Alito discussed historical expectations of society with regard to government surveillance of our movements:

> Society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[6]

The ACLU and others have expressed concern that ALPR systems potentially pose similar risks, particularly if deployed and used on a mass scale and pervasively across jurisdictional boundaries.[7] Not only actual government surveillance, but perceived government surveillance as well, can have a chilling effect on Americans' protected rights of free expression, free association, protest, political participation, and even our right to visit locations which some might find controversial or embarrassing.

Protecting Privacy and Civil Liberties

The NCRIC ALPR Policy, and the deployment of access control, auditing, revisioning, and data correction and purging technologies, applied to the privacy and civil liberties concerns articulated herein, will provide increased protection for data currency and accuracy, thereby helping to mitigate risks of misidentification, misuse of non-relevant information, and poor data quality. Concepts of proportionality, authorized use, accountability, and other policy and technical controls, will be incorporated, to deter,

---

International Association of Chiefs of Police, served as a primary information source for this Initial NCRIC PIA) (http://www.aclu.org/blog/tag/license-plate-scanners)

[5] American Civil Liberties Union of Iowa website discussion of Automatic License Plate Readers (ALPRs) in Iowa (http://www.aclu-ia.org/automatic-license-plate-readers-aplrs-in-iowa/)

[6] *United States v. Jones* 132 S.Ct. 945, 964 (2012).

[7] *See, e.g.,* "You Are Being Tracked. How License Plate Readers Are Being Used to Record Americans' Movements." American Civil Liberties Union, New York, NY, July 2013, (http://www.aclu.org/alpr)

detect, and control against misuse of ALPR Data reasonably likely to implicate these types of societal concerns.

Privacy and Civil Liberties Protections for NCRIC ALPR Data

Although extensive privacy policies already are in place, the NCRIC recognizes that ALPR Data has unique attributes that must be addressed through additional measures.

From its inception, the NCRIC has taken the issue of privacy and civil liberties seriously. To that end, the NCRIC follows the Information Privacy Policy adopted by the California State Terrorism Threat Assessment System (STTAS Privacy Policy)[8], which includes one State Fusion Center, four Regional Threat Assessment Centers and one Major Urban Area Fusion Center. The STTAS Privacy Policy was developed primarily to address the use and handling of criminal intelligence and related information as governed by 28 C.F.R. Part 23, the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files, and other applicable legal authorities.

To the extent individual elements of the STTAS Privacy Policy are applicable to ALPR Data, the NCRIC will adapt these elements to its handling of such data.

The NCRIC recognizes, however, that the use of ALPR and other locational data may, in some cases, present privacy and civil liberties challenges and protective requirements different from those addressed in the STTAS Privacy Policy and, as appropriate, the NCRIC will develop and implement additional protections. In addition, the NCRIC will adapt, to the extent reasonably feasible, the Fair Information Principles described in the STTAS Privacy Policy to the handling of ALPR Data. These principles include:

1. Collection Limitation;
2. Data Quality;
3. Purpose Specification;
4. Use Limitation;
5. Security Safeguards;
6. Openness;
7. Individual Participation; and
8. Accountability

Compliance with Applicable Law

As a threshold matter, and as mandated by the STTAS Privacy Policy, the NCRIC, and all

[8] As of the date of release of this document, the "STTAS Privacy Policy" title has not yet been revised to reflect the renaming from State Terrorism Threat Assessment System (STTAS) to State Threat Assessment System. Hence, all references to the policy preserve the "STTAS" acronym, while references to the organization use the modified "STAS" acronym.

assigned or detailed personnel, including personnel providing information technology services, private contractors, and other authorized participants in the NCRIC or any other STTAS Component, shall comply with all applicable laws protecting privacy, civil rights, and civil liberties.

Use for Authorized Law Enforcement and Public Safety Purposes Only

ALPR Data will be used only for authorized law enforcement and public safety purposes. Approved users are authorized to access ALPR Data to:

- Locate stolen, wanted, and subject of investigation vehicles;
- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;
- Locate witnesses and victims of violent crime;
- Locate missing children and elderly individuals, including responding to Amber and Silver Alerts;
- Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;
- Protect participants at special events; and
- Protect critical infrastructure sites.

Consistent with the NCRIC ALPR Policy to be further developed over the coming months, information sharing, access control, and use control technology will be utilized to: (1) record and audit the authorized use for which ALPR Data is being accessed or used in each instance; and (2) incorporate measures designed to prevent attempted access or use of ALPR Data for non-authorized purposes.

Collection of ALPR Data

NCRIC receives ALPR Data from its partner entities, but also operates a limited number of ALPR units. Such NCRIC ALPR units may be used to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

Dissemination, Secondary Uses, and Commercial/Private Entity Data Sharing

NCRIC ALPR Data will be disseminated only to authorized law enforcement or public safety officials with proper authority, for authorized purposes, and as consistent with standing Memoranda of Understanding (MOUs) or as otherwise authorized by source agencies. The NCRIC ALPR Policy will incorporate controls on secondary uses of ALPR Data. Information sharing, access control, and use control technology will be utilized to enforce and audit these requirements.

ALPR Data may be shared with owners or operators of critical infrastructure locations in circumstances where reasonable evidence suggests the location is the target of a terrorist attack or other criminal activity.

Except as noted above with regard to critical infrastructure, the NCRIC will not share NCRIC or partner agency ALPR Data with commercial or other private entities or individuals.

Safeguarding and Protecting ALPR Data

The NCRIC will take all reasonable physical, technological, administrative, procedural, and personnel measures to protect the confidentiality and integrity of ALPR Data, whether in storage or in transit.

Data Quality and Accuracy

The NCRIC will take all reasonable measures to ensure that ALPR Data is accurate and up-to-date. When errors are discovered, corrections will be made promptly and reasonable efforts will be taken to identify, locate, and update information that has been shared with other entities pursuant to the dissemination policy.

Data Vetting and Decision Making

The NCRIC ALPR Policy will establish policies and guidelines requiring human evaluation and verification in determining the relevance of license plate data to an active investigation or other authorized law enforcement or public safety effort. To the greatest extent feasible, ALPR data utilized in investigations will be corroborated by other information prior to using such data as the basis for subsequent law enforcement action.

Data Retention and Destruction

While continuing to refine its ALPR Policy, the NCRIC will incorporate reasonably feasible procedural and technological measures to enforce data retention and destruction requirements imposed by the originators of data received and electronically stored by the NCRIC. The NCRIC will collect and analyze empirical data to support an evaluation of reasonable retention standards for ALPR Data. During this period of analysis, the NCRIC will adopt a default, system-wide, one-year retention standard under which ALPR Data received from contributing agencies will be purged. Under these standards, if such data does not meet established retention requirements based on relevance to an ongoing criminal investigation (for which other retention standards may apply), it will be removed entirely from NCRIC databases.

Utilizing data gathered over the next year to evaluate the use and efficacy of ALPR Data, and based on consultations with privacy and civil liberties experts, the NCRIC will continue to develop and refine specific ALPR data retention and destruction policies, with additional restrictions applied based upon the intended authorized use. For example, further restrictions on temporal, geospatial, relational, and other factors may be implemented.

According to a recent survey,[9] albeit with a relatively small number of voluntarily responsive agencies, retention periods for ALPR Data vary widely, from none to infinite, with 46% retaining ALPR Data for one year or less, 13% between two and five years, and 14% indefinitely. Utilizing sophisticated analytic software, the NCRIC will consider, in consultation with member entities, the efficacy of ALPR Data of various ages in determining its data retention and destruction requirements.

Training and Non-Disclosure Obligations of NCRIC Personnel

All personnel with access to NCRIC ALPR Data will be provided with appropriate training, including privacy and security training, and will be required to sign non-disclosure agreements with regard to ALPR Data, as well as other information to which they will have access at NCRIC.

Auditing and Accountability

All NCRIC personnel with access to ALPR Data will be responsible for strict compliance with the NCRIC ALPR Policy, and all other applicable legal, regulatory, and policy requirements. The NCRIC will employ auditing technologies to enable tracking of, and accountability for, individual NCRIC participant actions to access, use, disseminate, retain, and/or destroy ALPR Data. Violations of applicable requirements will result in appropriate disciplinary action, including, if appropriate, denial of additional access to NCRIC facilities and data.

Updates and Revisions to the NCRIC ALPR PIA

This is an initial Privacy Impact Assessment only. It will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing, and other relevant considerations. Additionally, updates to this Privacy Impact Assessment may be used to inform continued refinements to the NCRIC ALPR Policy.

---

[9] *ALPR Systems Policy Operational Guidance for Law Enforcement,* International Association of Chiefs of Police, 2012, at 29 (http://www.theiacp.org/portals/0/pdfs/IACP_ALPR_Policy_Operational_Guidance.pdf)

DRAFT POLICY

Public Safety Camera Systems

378.1 PURPOSE AND SCOPE

This policy applies to all Police Department maintained public safety cameras that have monitoring and/or recording capabilities. Its purpose is to manage the use of public safety cameras in public places and to enhance public safety in a manner consistent with legal privacy rights.

378.2 GENERAL PRINCIPLES

(a) The principle objectives of public safety camera monitoring and/or recording are to:

1. Enhance existing public safety strategies, plans and initiatives;
2. Prevent and deter crime and public disorder;
3. Reduce the fear of crime;
4. Identify criminal activity and suspects;
5. Identify and gather evidence;
6. Document police actions to safeguard the rights of the public and police officers;
7. Reduce the cost and impact of criminal activities to the community;
8. Improve the allocation and deployment of law enforcement assets. Any use of public safety / security cameras that deviates from these principles is strictly prohibited by this policy.

(b) Public safety cameras monitoring and/or recording must be conducted in a professional, ethical, and legal manner. Personnel using the public safety camera system will be trained and supervised in the responsible use of the system. Violations of this policy and procedures may result in disciplinary action and subject those involved to criminal and/or civil liability under applicable state and federal laws;

(c) Information obtained through public safety camera video monitoring and/or recording will be used exclusively for safety, security, and other legitimate purposes and will only be released in accordance with this policy or as required by law;

(d) Public safety cameras that monitor and/or record public areas will be used in a manner consistent with all department policies, including the City's sexual harassment policy.

DRAFT POLICY

Public Safety Camera System

378.1 PURPOSE AND SCOPE

This policy applies to all Police Department maintained public safety cameras that have monitoring and/or recording capabilities. Its purpose is to manage the use of public safety cameras in public places and to enhance public safety in a manner consistent with legal privacy rights.

378.2 GENERAL PRINCIPLES

(a) The principle objectives of public safety camera monitoring and/or recording are to:

1. Enhance existing public safety strategies, plans and initiatives;
2. Prevent and deter crime and public disorder;
3. Reduce the fear of crime;
4. Identify criminal activity and suspects;
5. Identify and gather evidence;
6. Document police actions to safeguard the rights of the public and police officers;
7. Reduce the cost and impact of criminal activities to the community;
8. Improve the allocation and deployment of law enforcement assets. Any use of public safety / security cameras that deviates from these principles is strictly prohibited by this policy.

(b) Public safety cameras monitoring and/or recording must be conducted in a professional, ethical, and legal manner. Personnel using the public safety camera system will be trained and supervised in the responsible use of the system. Violations of this policy and procedures may result in disciplinary action and subject those involved to criminal and/or civil liability under applicable state and federal laws;

(c) Information obtained through public safety camera video monitoring and/or recording will be used exclusively for safety, security, and other legitimate purposes and will only be released in accordance with this policy or as required by law;

(d) Public safety cameras that monitor and/or record public areas will be used in a manner consistent with all department policies, including the City's sexual harassment policy.

Monitoring based solely on protected classifications (e.g., race, gender, sexual orientation, national origin, disability, etc.) is prohibited.

(e) Public safety camera monitoring of public areas, dwellings, and businesses is limited to uses that do not violate the reasonable expectation of privacy as defined by law.

378.3 PROCEDURE

(a) Public safety cameras will be monitored by personnel authorized by the Chief of Police or his/her designee. All public safety camera system operators must inspect the video monitors at or near the beginning of their shifts to ensure the system is functioning properly and that the system is recording correctly using the proper data/time stamp;

(b) An officer will be dispatched to any area in which a possible crime, motor vehicle accident, public safety risk, traffic incident, or other incident that necessitates police intervention is first observed using the public safety camera system. The responding officer will be the primary reporting officer of in-progress incidents.

(c) Public safety cameras will be used to observe locations that are in public view and where there is no reasonable expectation of privacy. Cameras will not be directed to look into adjacent, non-city owned buildings.

(d) Personnel will not continuously view or record people displaying affection in public areas, unless such activity is criminal in nature;

(e) Tampering with or duplicating recorded information without authorization is prohibited;

(f) Personnel shall not disseminate information obtained through the monitoring of public safety cameras unless such release complies with the law, this policy, or any other Police Department information-release policies.

(g) Public safety cameras should be clearly marked so as to be conspicuous to the general public and the location of each camera should be publically noticed at least 72 hours prior to installation. Public safety cameras should be positioned in a manner to avoid being vandalized.

(h) Public safety camera locations and fields of view shall be determined by the Chief of Police, and may include but shall not be limited to: Areas that in the Chief of Police's opinion maximize and enhance public safety; areas identified as "hot spots" for criminal activity; and/ or major thoroughfares into and out of the City. Placement of public safety cameras will also take into consideration physical limitations such as availability of power, cellular signal network reception and reasonable mounting facilities.

378.3.1 RESPONSIBILITIES

(a) The Police Department is the only City department authorized and responsible for the oversight and use of public safety cameras on behalf of the City. In addition to being responsible for all operational issues related to public safety cameras, the Police Department has primary responsibility for ensuring adherence to this policy and for disseminating the policy to persons requesting information on public safety camera policy and procedures.

(b) The Police Department is responsible for following new developments in relevant laws and security industry practices to ensure that public safety cameras monitoring and/or recording is consistent with the highest standards and protections.

(c) This policy does not create an affirmative duty upon the Police Department to monitor public safety camera equipment in public places on a continuous or periodic basis.

378.3.2 TRAINING/OVERSIGHT

All personnel operating the Public safety/ security camera system will be trained in the technical and legal parameters of appropriate system use.

(a) Personnel will be given a copy of this policy and will provide written acknowledgment that they have read and understood its contents;

(b) Personnel will receive yearly training to reinforce the importance of proper use of the system and to keep abreast of current law;

(c) All personnel involved in monitoring and/or recording public areas will perform their duties in accordance with relevant law and this policy;

(d) The Chief of Police or his/her designee(s) will ensure that responsible monitoring/recording practices are followed by conducting yearly audits. Such audits will include an inspection of the monitoring equipment, camera placement, maintenance logs, and incident documentation records.

378.3.3 RETENTION, EXTRACTION AND STORAGE PROCEDURE

(a) Recorded video images will be stored for a maximum of xx days. Images will be deleted after xx days unless the video footage must be retained as part of a police investigation, court proceeding, Professional Standards Unit Investigation, or their legitimate use as approved by the Chief of Police;

(b) All requests for a copy of video surveillance footage require the completion of a "Request for public safety camera video" form. This form must include the date of the request, a brief description of the request, including the reason for request nature of the

recording, incident case number, specific time frames, signature of the requesting officer, and the name of the extracting officer;

(c) Only personnel authorized by the Chief of Police or his/her designee are authorized to extract video footage from the system. Video monitors will not be placed in locations that facilitate public viewing. Video monitors and storage equipment will be kept in a locked and key controlled room.

(d) Video footage extracted onto digital media for investigative purposes shall be marked with the incident case number, the extracting officer's name and serial number, and the appropriate watermarking or system verification information. The digital media will then be given to the investigating officer and booked as evidence into the Property Room. The requesting officer is responsible for booking the digital media, including a copy of the "Request for public safety cameras video" form, into evidence;

(e) The only digital media recognized as authentic for legal or evidentiary purposes shall be the original extracted version booked into the Property Room. Officers and investigators shall not maintain the original extracted media with the incident case file; however, "working copies" of this media may be part of the file;

(f) A download log will be kept for all extracted footage along with the completed "Request for Public safety camera video" forms in the monitoring room.

(g) Purging of the system will be automatically set based on the retention period in section 387.3.3(a).

378.4 AUDITS

Audits will be conducted annually to ensure compliance with this policy. Completed audit reports will be forwarded through the public safety cameras manager and/or the Services Captain to the Chief of Police or his/her designee. Audit results that need further review may be forwarded to an ad-hoc board consisting of subject matter experts selected by the Chief of Police.

378.4.1 COMPLAINT PROCESS

All internal and external complaints related to the public safety camera system or this policy will follow standard complaint procedures as outlined in the Policy Manual, and applicable law.

378.5 ANNUAL REVIEW OF THE PUBLIC SAFETY CAMERA SYSTEM

The Chief of Police or his/her designee will conduct an annual review of the public safety camera system. The annual review will include an inventory of video monitoring installations, dates of installations, summary of the purpose, adherence to this policy and any proposed policy changes. The results of each review will be documented and maintained by the Chief of

Police or his/her designee and other applicable advisory bodies. Any concerns or deviations from this policy will be addressed promptly and effectively.

378.6 PUBLIC EDUCATION

The Chief of Police of his/her designee will provide public education materials on the video cameras, which may include public meetings, posting informational items on the City website, including this policy, and/or having informational flyers available to the public.

2128872.1

San Leandro Police Department • Proud to Serve

Chief's Advisory Board Meeting Notes
Tuesday, July 30, 2013

Community Crime Cameras –Discussion:

1. Purpose and Scope
2. General Principals
3. Procedures
4. Responsibilities
5. Training/Oversight
6. Retention/Extraction and Storage Procedure
7. Audits
8. Complaint Process
9. Annual Review of the Public Safety Camera System

- Concerns/Feedback
  - Free Standing Surveillance Systems throughout City (i.e. City Hall, Senior Center, Police Department)
    - IT Budgeted $240K to Replace Cameras in City Hall & Police Department
    - Community Camera Costs are Approximately $10-20K Per Camera
  - Reviewed Actual Scenarios where Technology Helped to Apprehend Suspects
  - Disciplinary Actions for Violating Policy
    - Discussion on Policy Violations
  - Concern about Data Storage – iCloud - Reducing Retention and Losing Frames (Data)
  - Access – Protected Room and Not Having Video Footage Monitored Unless Needed to Assist in Solving a Crime
    - Video Footage will be in a Locked Area
    - Access will be Given to Management (Chief, Captains, and Lieutenants)
      - Access will be Tracked/ Strict Monitoring – Audits in Place – As With Department of Justice and CLETS
      - All Extracted Video Footage will be Logged
  - Training – Require Signing Policy Annually & Yearly Training on Procedures
  - Definitions of "Law Enforcement" and "System Operator"
  - Providing Public Notification Before Community Cameras are Installed – 30 Days
  - Discussion on Number of Community Cameras and Locations
  - Concern that Cameras will Not Reduce Crime.
    - Goals are: Prevention of Crime & Provide Safety to Community
  - Performance Measures – Results/Measure Success/ Impact on Crime
    - Discussed Newly Implemented Crime Suppression Unit
      - Feedback from Police Department/Community
      - Impacting Crime/ Targeting Hotspots
      - 2 Months Steady Decline in Crime Since Implementation
  - Importance of Crime Intel/Debriefing Criminals/Collecting & Information Sharing
  - Request to Speak to District Attorney Regarding Discovery Process

- Chief's Advisory Board Vote – Implementation of Community Cameras
  - 81% - Yes, In Favor of Installing Cameras
  - 13% – Not in Favor of Installing Cameras
  - 6% Undecided – Need Additional Information
- Emphasis that Video Footage Cannot be Accessed by City Staff/Regulation by Law
  - Data Housed at SLPD/Cameras Not Linked to Outside Access
  - Existing Auditing Procedure in Place
- Discussion on Government Code – Retention Policy 1 Year
- A Follow Up Meeting will be Scheduled to Continue Discussion
  - Meeting Scheduled Monday, August 12, 2013 at 4:00 p.m.

Public Safety Initiative "United For Safety" Outcomes

- Event Well Attended – Approx. 1,000 Attendees - Positive Feedback From Community
- Donations for Beverages, Food, and Raffle Prizes
- KTSF Came to Event and Interviewed Community Members
- San Leandro Police Department Debriefed Event – Collected Feedback for Next Year
- CalChief's Article

Feedback on Oral Board – Lieutenant Exam

- Process has Been Re-Designed to Include Community Members and Outside Agencies on Panel Interviews
- An Independent Contractor Facilitates the Testing Process
- Chief's Advisory Board Members Peggy McCormick & Michael Fitzgerald Participated
  - Quality Candidates Interviewed for Lieutenant from SLPD
  - Testing Phase Included Mock/Community Interviews
  - Common Interest of All Candidates – Relationships with Public/Community is Important
  - Combination of Community Panel and External Law Enforcement is Essential for the Selection Process or Department Promotions

Animal Ordinance Update

- Plan Meeting with Community Members to Gather Feedback to Finalize Ordinance
- Develop Comprehensive Ordinance to Include Novice Beekeepers and Chicken Coops

K9 Competition

- The San Leandro Police Department and Alameda Police Department are hosting the First Annual Police K-9 Competition - Search, Agility, Obedience, and Protection.
  - Saturday, August 3, 2013 9:00 a.m. - 1101 West Red Line Avenue, Alameda,

Adjournment 7:05 p.m.

San Leandro Police Chief Advisory Board Camera Policy Assignment 7-2013

	Comments With Some Questions
1.	I believe that putting surveillance cameras in residential areas will help keep San Leandro safer but I will agree with what xxxx mentioned about "Big Brother" happening. That's something I don't agree with. I also asked some of my peers about it as well and they all agreed that your idea will help San Leandro become Safer.
2.	I was wondering where will the cameras be located at? The light post? Because anybody can be able to vandalize it if it was at lower ground levels.
3.	Must educate the public that the cameras will help prevent crime as in other cities. The police dept must be completely transparent with the use and it should be noted that they will be put in public locations only.
4.	I think the police team should conduct a series of public educational lessons on the advantages of camera and showcase statistical data to residents on how cameras fight crime. A Committee or the CAB should have some oversight and governing power to guide Police decisions.
5.	Is the Department contracting Lexipol? If yes, what are their policy recommendations?
6.	Are more resources available to us? A report or presentation on public surveillance systems? It would be helpful for us to have good overview and better understanding? Any laws and legislation we need to know about? Are there evaluations from other cities (lessons they learned?)
7.	Budget and cost analysis would be helpful. Equipment, installation, implementation, use (active staff monitoring or passively monitored), ongoing maintenance, storage. Should also factor in potential future upgrades and/or expansions.
8.	Transparency is key and very important. Community outreach, public meetings. Input from businesses and interest groups (are there any groups we should be aware of?)
9.	Any changes must be brought to public forums for discussion and for the public to allow or disallow, including usage policies of current surveillance, sharing of data, changes in data retention, access, releases to any other organizations, and all uses of the data by our own organizations or those the data is shared with.
10.	That outside independent entities without conflict of interest be selected by the civil government of San Leandro to guide the decision making process based on the data available.
11.	The policy requires a three (3) pronged oversight committee. The committee should include judicial oversight, citizen review, as well as a strong law enforcement component. The program, policy and committee should be impartial and transparent providing regular and open reports to the City Council. The policy should contain serious commonsense rules that are easily applied to meet the requirements of police, judiciary and citizens.
12.	There should be strict limits on surveillance to protect citizen privacy, limits on targeting individuals, time limits on storage and a clear understanding of where data is being stored and with whom it is being shared, what their time limits are and with whom they share information.

13.	Any surveillance program should take advantage of the technical innovations available to us in San Leandro. The initial goal should be aimed at being the best possible system, with the ability to easily improve and upgrade. As well, the program should include a funding source from beginning development, taking into account the need for regular upgrades.
14.	Need a definite retention time period for normal (non criminal) recordings and destruction and detail of destruction process, records and personnel responsible. 2. A definitive process and who/whom will determine the placement of the cameras. Note, according to the California Government Code Section 34090.6 regarding electronic recordings, I do not see that this or any other section of the California Government Code will apply as long as our cameras do not record sounds (conversations) and the policy and SOP are approved by the City Council. It appears that we are flexible to write a our own policy without State restrictions.

Below I have included additional information for the Board from one of the Board Members. I wanted to respect the Board Members time and effort to educate the Board, so I have included it as additional reading if you choose.

The following feedback is on the larger issues and the sample law.

Surveillance technology has an extremely poor record when it comes to authorities abusing the technology in illegal, immoral, and damaging ways. These actions not only compromise the rights of the residents and individuals, but undermine the trust of those within the purview of those departments. There is little evidence to support their effectiveness when one takes into account larger views of the geographic region. In fact, some municipalities have removed them once in place due to the ill effects and lack of effectiveness and reducing crime.

The sample law provided leaves me with several concerns, but none of them so much as the fact that the law is written in such a way as to allow virtually any use of the information gathered and stored as nearly any "use" qualifies.

- There is no review over the selection of locations beyond that of the Chief of Police, nor any criteria as to why locations will be selected.
- Recordings can be kept longer than one year for "official reasons" - This is undefined, but mentioned uses includes use of the information for civil cases, monitoring pedestrian and vehicle traffic, to "maintain public order", "provide effective services," and "improve the general environment". Given this, any and all information could be deemed to be kept for "official reasons" forever.
- Why is the information not available to the general public?
- This information can be made available to "other than police personnel" as designated by the Chief of Police with no limitations or requirement of notice.

San Leandro Police Chief Advisory Board Camera Policy Assignment 7-2013

Some references regarding the points made above:

Do security cameras deter crime?
Homeland Security News Wire, Feb 2011
http://www.homelandsecuritynewswire.com/do-security-cameras-deter-crime
"Even in the studies that show cameras help, the question arises: compared to what? Any **funds spent on this gadgetry cannot be spent on beat cops**, probation officers, laboratory gear or jail cells," he writes.
"**The challenge for enthusiasts is to show the technology outperforms other options.**"

Study Questions Whether Cameras Cut Crime
NYTimes, March 2009
http://cityroom.blogs.nytimes.com/2009/03/03/study-questions-whether-cameras-cut-crime/
...the other three studies, which ranged from 1978 to 2002 and focused on lower-crime situations, found that the cameras' impact on reducing crime was **statistically inconclusive**. And the researchers raise the **question whether the trade-offs in cost and loss of privacy are worth it**.

San Francisco Surveillance Cameras Don't Reduce Violent Crime, Study Finds
ACLU of N. CA, April 2009
https://www.aclunc.org/issues/technology/blog/san_francisco_surveillance_cameras_dont_reduce_violent_crime,_study_finds.shtml
In line with similar studies from around the world, the report found that San Francisco's **video surveillance cameras do not make people safer**. The cameras have **failed to prevent or reduce violent crime, including homicides**. The cameras have also had **no effect on drug offenses or prostitution**.

Cambridge halts activation of surveillance cameras
http://www.boston.com/news/local/massachusetts/articles/2009/02/04/cambridge_halts_activation_of_surveillance_cameras/
"**The City Council is not convinced that the proposed benefits will outweigh the potential risks**," said Cambridge Mayor E. Denise Simmons. The cameras were paid for with a $4.6 million grant from the US Department of Homeland Security.

Lansing Surveillance Cameras Are Costly, Ineffective and Invasive
ACLU Report, August 2012
http://www.aclu.org/national-security/lansing-surveillance-cameras-are-costly-ineffective-and-invasive-aclu-report-warns
A comprehensive study conducted by the UK found that its 4.2 million cameras did not reduce crime. In **Oakland, Calif., Police Chief Joseph Samuels, Jr. concluded that "...there is no conclusive way to establish that the presence of video surveillance cameras resulted in the prevention or reduction of crime.**" ...the City of Detroit approved one of the largest video

surveillance systems in the country, only to eliminate it 14 years later because the **high maintenance and personnel costs did not justify the minimal results**.

...the system of cameras **could be used to monitor peaceful protests and other constitutionally protected activities including the movements of innocent people throughout the city**. The private information collected by cameras is also **ripe for abuse**, the ACLU states, and could be used for **voyeurism, stalking, or harassment**. Furthermore, an independent study of the cameras conducted by a researcher at Oakland University concludes that **African American residents of Lansing are twice as likely to be under constant surveillance** in their neighborhoods as white Lansing residents.

Surveillance Camera Policy –

Policy number 378, the Public Safety Camera System, as submitted by Chief Spagnoli is a good starting point for the City of San Leandro as they develop their own policy; however, I believe the policy could be strengthened with following recommendations:

1. Unless limited by technological constraints, camera recordings shall be stored electronically for a period of not less than ten days. The system shall be configured to automatically purge and write over any recordings more than 10 days old. * *Note: 100 days seems way too long. Best practice seems to dictate 10 days of recording.*
2. Cameras should be clearly marked so as to be conspicuous to the general public and the location of each camera shall be made public at least 72 hours prior to installation.
3. A review board and or an independent annual audit of the camera system should be implemented to ensure adherence to policy and to ensure placement of each camera meets the objectives outlined and maximum utilization of each camera is obtained.

City of San Leandro

Meeting Date: September 3, 2013

Minute Order - Council

File Number: 13-450 **Agenda Section:** ACTION ITEMS

Agenda Number:

TO: City Council

FROM: Chris Zapata
City Manager

BY: Sandra Spagnoli
Chief of Police

FINANCE REVIEW: Not Applicable

TITLE: MOTION: Motion Directing Staff to Include Community Cameras in the Public Safety Camera Project