Automated License Plate Reader System

450.1 PURPOSE AND SCOPE

Frequently the Central Marin experiences patterns of criminal activity perpetrated by both residents and non-resident criminals. Most of this criminal activity involves theft from vehicles, burglaries and auto thefts. The Police Authority staff has determined that deployment of an Automated License Plate Reader System (ALPRS) would be a desirable and cost effective resource for suppression of these crimes. The Police Authority has concluded that such a system will enhance public safety in the City of Larkspur, the Town of Corte Madera, and the Town of San Anselmo.

It is the intent of the Police Authority to:

1. Ensure that ALPRS is capable of effectively and efficiently achieving its articulated purpose.

2. Ensure that the design, scope and capabilities of the ALPRS minimize its negative impact on privacy.

3. Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system which complies with current California and Federal laws.

450.2 POLICY

The Central Marin operates an ALPRS as an investigative resource for the sole purpose of creating a safer environment and community for all those who live, work and visit our jurisdiction. This policy provides guidelines for ALPRS operation

450.3 DEFINITIONS

450.3.1 ALPRS

A portable and non-portable, fixed system consisting of a camera, or cameras, and related equipment used to capture, record, transmit and store license plate and vehicle images/data recorded on public spaces for use in criminal investigations; and for searching data files for vehicles wanted or sought in connection with the commission of a serious crimes; and capable of promptly notifying the Police Authority of the presence of such vehicles in our jurisdiction.

450.4 EQUIPMENT AND LOCATIONS

ALPRS cameras used by the Police Authority will be in fixed or mobile locations in public space approved by the Chief of Police. These cameras will be positioned to only record rear or front images of vehicles and their license plates. These cameras will not have pan, tilt and zoom capabilities or the ability to record sound. These cameras will not be installed in, or directed at any space where a reasonable expectation of privacy exists.

Adoption Date: 2016/02/11

450.5 USER ACCESS

Images/data will be continuously recorded. Images/data will be transmitted and stored to a dedicated computer at the Northern California Regional Intelligence Center (NCRIC) for one year. NCRIC mission is to safeguard the community by serving as a dynamic security nexus for local Bay Area law enforcement agencies. CMPA and NCRIC determined that it would be mutually beneficial to cooperate and coordinate in providing the highest level of public safety to the public, guided by the principle that performing cooperatively is in the best interest of the public.

Access to the images/data will be limited to police officers and detectives. Access is for the sole purpose of identifying vehicles suspected of being occupied or operated by person(s) responsible for crimes under investigation by the Police Authority or other law enforcement agencies.

Access will require a unique login/password for each authorized user of the system. User names and passwords will be issued by the designed system administrator to individuals approved by the Chief of Police. The system will record user access for audit purposes.

Real time access and viewing may be authorized by the Chief of Police, the Police Lieutenant or the watch Commander to facilitate emergency traffic or disaster management, or when it is reasonable to believe such use may result in the apprehension of an at large felony suspect known or suspected of being in or en-route to our jurisdiction.

450.6 TRAINING

Personnel authorized to access the ALPRS will be appropriately trained and supervised in use of the equipment and this policy. There should be annual department training regarding the access and use of ALPRS programs and equipment.

450.7 PROHIBITED ACTIVITY

System use shall be conducted in a professional, ethical and legal manner. The ALPRS will not be used for any purpose not directly related to a criminal investigation, a reported crime, or disaster management.

450.8 IMAGE/DATA STORAGE

All images/data will be stored in a secure area with access restricted to authorized persons except that images/data retained in connection to a criminal investigation shall be transferred to suitable storage medium and placed into evidence in accordance with current departmental evidence procedures.

CMPA and NCRIC have entered into a Memorandum of Understanding (MOU) designating NCRIC as the host for CMPA motor vehicle license plate recognition information and informational technology services. CMPA and NCRIC agree to enforce and maintain security requirements for the information stored in the ALPRS data repositories as specified in the Information Practices Act, the Public Records Act, California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files and Criminal Intelligence Operational Activities, and 28 Code of Federal Regulations (CFR) Part 23.

450.9 RELEASE OF IMAGES

The release of images/data shall be done only with the authorization of the Chief of Police or the Police Lieutenant, or in compliance with a search warrant, subpoena, court order or in accordance with a federal or California statute. Images/data released under such conditions shall be transferred to a disc and placed into evidence and released in accordance with current departmental evidence procedures under the supervision and control of the Evidence Technician.

450.9.1 ALLIED AGENCY INVESTIGATIVE REQUESTS

Requests for images/data from other government agencies required for a criminal investigation shall be submitted to the Investigative Sergeant, who will promptly review the request for conformity with this policy before any release. The images/data requested shall be preserved until the request has been reviewed. Release of any images will be in accordance with current departmental evidence procedures and California state law.

450.9.2 PUBLIC RECORDS ACT REQUESTS

Images/data captured by ALPRS are exempt from release pursuant to the California Public Records Act (CPRA) Government Code Section 6254.

450.10 ANNUAL REVIEW OF THE ALPRS

The Chief of Police or his/her designee should conduct an annual review of the ALPRS. The annual review will include an inventory of all ALPRS related equipment, annual system costs and a summary of any policy violations, or a statement of compliance with the established policy.

NCRIC Automated License Plate Reader Policy

NCRIC MISSION

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.

AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGIES

To support authorized law enforcement and public safety purposes of local, state, federal, and tribal public safety agencies, the NCRIC utilizes Automated License Plate Reader (ALPR) technology, and supporting software, to gather and analyze ALPR data to enable the rapid identification and location of vehicles of legitimate interest to law enforcement. ALPR units are attached to law enforcement vehicles or deployed at fixed locations, where they collect license plate information from vehicles on public roadways and public property. In one common use of ALPR technology, license plate encounters are compared against law enforcement "hotlists" – lists of vehicles associated with active investigations, for example, related to Amber Alerts or other missing children, stolen vehicles, or stolen license plates. The information is also retained for a fixed retention period, though it is only re-accessible by law enforcement given a legitimate law enforcement purpose as listed below.

PURPOSE

This NCRIC Automated License Plate Reader Policy (ALPR Policy) defines a minimum set of binding guidelines to govern the use of Automated License Plate Reader Data (ALPR Data), in order to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties.

The NCRIC also completed a NCRIC ALPR Privacy Impact Assessment (PIA) to address in further detail common privacy and civil liberties concerns regarding Automated License Plate Reader technology. The current version of this document is available on the NCRIC web site at www.ncric.org.

AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA

To support the mission of the NCRIC, Law enforcement personnel with a need and right to know will utilize ALPR technology 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.

RESTRICTIONS ON COLLECTION OF ALPR DATA AND USE OF ALPR SYSTEMS

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.

ALPR operators may not contact occupants of stolen, wanted, or subject-of-investigation vehicles unless the ALPR operators are sworn law enforcement officers. ALPR operators must rely on their parent agency rules and regulations regarding equipment, protection, self-identification, and use of force when stopping vehicles or making contact.

ALPR operators must recognize that the data collected from the ALPR device, and the content of referenced hotlists, consists of data that may or may not be accurate, despite ongoing efforts to maximize the currency and accuracy of such data. To the greatest extent possible, vehicle and subject information will be verified from separate Law enforcement information sources to confirm the vehicle or subject's identity and justification for contact. Users of ALPR Data must, to the fullest extent possible, visually confirm the plate characters generated by the ALPR readers correspond with the digital image of the license plate in question.

All users of NCRIC ALPR equipment or accessing NCRIC ALPR Data are required to acknowledge that they have read and understood the NCRIC ALPR Policy prior to use of the ALPR System.

In no case shall the NCRIC ALPR system be used for any purpose other than a legitimate law enforcement or public safety purpose.

TRAINING

Only persons trained in the use of the NCRIC ALPR system, including its privacy and civil liberties protections, shall be allowed access to NCRIC ALPR Data. Training shall consist of:

- Legal authorities, developments, and issues involving the use of ALPR Data and technology
- Current NCRIC Policy regarding appropriate use of NCRIC ALPR systems;
- Evolution of ALPR and related technologies, including new capabilities and associated risks;

- Technical, physical, administrative, and procedural measures to protect the security of ALPR Data against unauthorized access or use; and
- Practical exercises in the use of the NCRIC ALPR system

Training shall be updated as technological, legal, and other changes that affect the use of the NCRIC ALPR system occur. In no case shall a person utilize the NCRIC ALPR system if he/she has not completed training in more than a year.

AUDIT

Access to, and use of, ALPR Data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- The name of the law enforcement user;
- The name of the agency employing the user;
- The date and time of access;
- The specific data accessed;
- The supplied authorized law enforcement or public safety justification for access; and
- A case number associated with the investigative effort generating the ALPR data query.

Audit reports will be provided periodically and on request to supervisory personnel at the NCRIC and partner agencies.

In addition, no less frequently than every 12 months, the NCRIC will audit a sampling of ALPR system utilization from the prior 12 month period to verify proper use in accordance with the above authorized uses. Any discovered intentional misconduct will lead to further investigation, termination of system access, and notification of the user's parent agency for appropriate recourse. In addition, the auditing data will be used to identify systemic issues, inadvertent misuse, and requirements for policy changes, training enhancements, or additional oversight mechanisms.

These ALPR audits shall be conducted by a senior NCRIC official other than the person assigned to manage the NCRIC ALPR function. Audit results shall then be reported to the Director of the NCRIC.

DATA QUALITY AND ACCURACY

The NCRIC will take reasonable measures to ensure the accuracy of ALPR Data collected by NCRIC ALPR units and partner agency ALPR systems. Errors discovered in ALPR Data collected by NCRIC ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question. Errors discovered in ALPR Data collected from partner agencies' ALPR systems are communicated back to the controlling agency to be addressed as deemed appropriate by that agency or in accordance with the agency's own ALPR data policies.

As the downstream custodian of "hotlists", the NCRIC will provide the most recent versions of these lists available and ensure the lists are refreshed from state or federal sources on a daily basis.

The NCRIC acknowledges that, in rare instances ALPR units may inadvertently capture information contrary to the collection guidelines set forth in this policy. Such records will be purged upon identification. Any discovered notable increase in frequency of these incidents from specific ALPR units or agencies will be followed up with for equipment repairs, camera realignment, or personnel training as necessary.

PHYSICAL AND ELECTRONIC SECURITY OF ALPR DATA:

Data collected by ALPR systems is stored in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff in good standing who have completed background investigations and possess an active security clearance at the "SECRET" or higher level.

NCRIC will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

RETENTION OF ALPR DATA:

ALPR Data collected by NCRIC ALPR units or shared from partner agencies' ALPR units shall not be retained longer than 12 months, or the length of time required by the partner agency who is custodian of the record – whichever is shorter. Once the retention period has expired, the record will be purged entirely from all active and backup systems unless a reasonable suspicion has been established that the vehicle identified by the ALPR read is connected to criminal activities.

ALPR records matching an entry in a current law enforcement hotlist will trigger an immediate notification to the officer operating the ALPR unit, the active dispatch officer at the agency owning the ALPR unit, the NCRIC, and the custodial agency of the hotlist. Such notifications are also subject to a maximum retention of 12 months.

ALPR Data obtained with license plate information not appearing on hotlists, and with no immediate reasonable connection to criminal activity, will be retained in secure systems so as to only be made accessible to authorized personnel for a maximum period of twelve months, then purged entirely from all systems. If during the specified retention period there is information which supports a legitimate law enforcement purpose (see above section enumerating AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA) as to a license plate or partial license plate which was recorded and is retained in these systems, then limited access will be permitted for predicate-based querying for potential matches against the parameters specific to the legitimate law enforcement purpose. Such events shall

be recorded in an access log showing date, time, name of person seeking access, agency of employment, reason for access, and tracking identifiers such as an agency case number.

ALPR records of vehicles having been identified and linked to criminal investigation will be entered into the relevant NCRIC database(s) and retained for a period of no more than five years. If during the five-year period NCRIC personnel become aware that the vehicle license plate information is no longer associated with a criminal investigation, it will be purged from the NCRIC's databases.

CUSTODIAN OF RECORDS AND RECORDS REQUESTS

Each agency sharing data retains control and ownership as the official custodian of its records, and must independently verify all external information obtained via NCRIC Information Systems. To the extent permitted by law, requests for information under the California Public Records Act or Freedom of Information Act or similar applicable laws will be directed back to the owner of the requested data.

SYSTEM MANAGEMENT AND ACCOUNTABILITY

The NCRIC shall assign a senior officer who will have responsibility, and be accountable, for managing the ALPR Data collected and ensuring that the privacy and civil liberties protection and other provisions of this ALPR Policy are carried out. This individual shall also be responsible for managing a process for maintaining the most current and accurate hotlists available from NCRIC law enforcement sources. This individual shall also have the responsibility for the security of the hotlist information and any ALPR Data which is maintained by the NCRIC. It remains, however, the personal responsibility of all officers with access to ALPR Data to take reasonable measures to protect the privacy and civil liberties of individuals, as well as the security and confidentiality of ALPR Data.

COMMERCIALLY CREATED ALPR DATA

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

DISSEMINATION

The NCRIC may disseminate ALPR data to any governmental entity with an authorized law enforcement or public safety purpose for access to such data. The NCRIC assumes no responsibility or liability for the acts or omissions of other agencies in making use of the ALPR data properly disseminated. Though the NCRIC will make every reasonable effort to ensure the quality of shared ALPR Data and hotlists, it cannot make absolute guarantees of the accuracy of information provided.

ALPR Information may be disseminated to owners and operators of critical infrastructure in circumstances where such infrastructure is reasonably believed to be the target of surveillance for the

purpose of a terrorist attack or other criminal activity. In these situations, the NCRIC also will make notification to appropriate local, state, and federal law enforcement agencies.

Information collected by the ALPR system shall not be disseminated to private parties, other than critical infrastructure owners or operators, as limited above, unless authorized, in writing, by the Director of the NCRIC or his designee. ALPR information shall not be disseminated for personal gain or for any other non-law enforcement purposes.

POLICY REVISIONS

NCRIC ALPR Policies 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 agreements, and other relevant considerations.

The most current version of the ALPR Policy may be obtained from the NCRIC website at http://www.ncric.org/