Automated Regional Justice Information System (ARJIS)
Acceptable Use Policy for the Regional License Plate Reader System

Revised: 02/13/2015

A. STATEMENT OF PURPOSE

The purpose of this document is to outline the responsibilities of the Automated Regional Justice Information System (ARJIS) in its role as a law enforcement information technology provider for the Regional License Plate Reader (LPR) data storage system (LPR system). ARJIS, in cooperation with local, state, and federal law enforcement agencies, maintains a regional server as a LPR data repository in support of law enforcement efforts to improve public safety.

ARJIS provides the secure network infrastructure, technical standards, security protocols, controlled access, and database administration for the LPR system. Included in the support of the secure infrastructure are ongoing system updates, maintenance, disaster recovery, and security monitoring of the circuits, hubs, routers, firewalls, databases, and other components that comprise the ARJIS Enterprise, ensuring the priority, integrity, and availability of service to authorized law enforcement users. This Acceptable Use Policy sets forth rules restricting how the LPR system may be accessed by authorized user agencies (agencies) and defines how the LPR system is maintained by ARJIS.

The Regional LPR Operational Protocol under development by the County Chiefs' and Sheriff's Association outlines LPR best practices and standard operating procedures for those agencies that utilize LPR in the field.

B. LPR OVERVIEW

LPR data is collected by agencies utilizing specially-designed cameras to randomly capture an image of a vehicle license plate and convert the plate characters into a text file using optical character recognition technology. The text file can then be sent to a computer and compared against pre-existing data files, such as databases containing records of stolen or wanted vehicles as well as vehicles associated with AMBER alerts, missing children, wanted subjects, or other criteria. If a match is found, the LPR user (law enforcement officer or agency) is notified by an audible alert and an associated notation on the user's computer screen.

LPR cameras can be mobile (mounted on vehicles) or fixed (mounted to a structure) as determined by the agency that owns the cameras.

Mobile LPR systems scan plates, notify the user of a vehicle alert, and store the plate scan data for upload or transfer to an agency LPR server or the regional LPR server. LPRs in fixed positions link to an LPR server at the agency owning the fixed camera for updates, transmission of scanned plate data in real- time or near-real time, and alert notifications. The LPR data from agency LPR servers is replicated (copied) to the regional server in near real time. The alerting functionality resides with the agencies, not with ARJIS.

The alert lists against which license plate reads are checked may include (but are not limited to) the Stolen Vehicle System and Felony Warrants System, provided by the California Department of Justice (Cal DOJ); and downloaded four times a day. LPR users are required to take into account the potential for lag time between the last update and an alert provided by the LPR system on a stolen or wanted vehicle. Any alert provided by an LPR system is to be considered informational and advisory in nature only and any subsequent action in the field will be based on a law enforcement

agency's standard operating procedures.

1. Specification of Use

Recognizing the public safety benefits that could be achieved by the effective sharing of LPR data, ARJIS established a regional server accessible to authorized agencies capable of receiving and storing LPR data as well as providing query and alerting functions. The data is transferred to the regional server via wireless or hard-wired encrypted communications. Some of the agencies send their scanned plates directly to the regional server, while most of the larger agencies send their LPR scans to their agency-specific server first. The data is then uploaded to the regional server, in near-real time.

The plates scanned by the LPR systems are stored in a stand-alone regional server. The regional server is designed to meet Federal Bureau of Investigation Criminal Justice Information System (FBI CJIS) and Cal DOJ requirements, policies, and procedures, and is not connected to any other server.

The LPR system is restricted to legitimate criminal justice uses for the purpose of furthering law enforcement goals and enhancing public safety. There are two primary objectives of LPR data use in the region. The first is to identify stolen or lost vehicles and license plates, and wanted or missing persons, by matching the LPR data to the alert lists downloaded by Cal DOJ. The second objective is the ability to query LPR data to assist officers with ongoing criminal investigations, crime prevention and detection, and aid in the prosecution of crimes involving vehicles. LPR data is queried only if there is a reasonable suspicion that a vehicle is involved in criminal activity and the requestor has a legitimate need to know.

2. Privacy and Data Quality

2a. Privacy

In October 2008, prior to the implementation of the LPR system, ARJIS participated in a Privacy Impact Assessment (PIA) effort led by the International Association of Chiefs of Police. This effort involved the review of existing local, state, and federal laws, and American Civil Liberties Union privacy concerns. The resulting PIA, published in 2009, provided background for the development of this Policy.

Access to and use of LPR data is for official law enforcement purposes only. Accessing and/or releasing data from the LPR system for non-law enforcement purposes is prohibited. LPR data access and use is governed by the Cal DOJ California Law Enforcement Telecommunications System (CLETS) Polices, Practices and Procedures (PPP) (current rev. 09/2014), via CalMaster Control Agreement between the San Diego County Sheriff's Department (Sheriff) and ARJIS. The CLETS PPP further references the FBI CJIS Security Policy (current rev. 5.3, 8/4/2014).

The data records stored on the regional LPR server include photographs of the vehicle (close-up of the license plate and context photo of the rear of the vehicle)

and accompanying license plate number, date, time, and location in the field, and do not directly identify a particular person.

2b. Source Data

Each agency contributing data retains control and ownership as the official custodian of its records. Prior to sending any data to the regional LPR database, an agency must comply with the following:

- Be an ARJIS Public Safety member agency.
- Be a CLETS-certified agency.
- Be the owner, operator, manager, or controller of the LPR equipment that captures the contributed data.
- Maintain compliance with applicable FBI CJIS security policies regarding law enforcement data.
- Provide only LPR data that is in a format consistent with the National Information Exchange Model (NIEM) standard, or data that is readily capable of conversion to a NIEM-compliant format.
- Provide LPR data that includes, at a minimum, the time, date, and location of capture as well as a unique identifier of the equipment used to capture the information.
- Ensure that LPR equipment utilized by the agency is in full compliance with any requirements or standards established by the United States Department of Justice in regard to LPR systems.
- It is recommended that agencies that do not operate their own LPR server will implement a real time or near-real time data transfer to the regional server, via encrypted communication infrastructure, approved by Cal DOJ. This ensures the timeliness and effectiveness of the alert lists and provides maximum public safety benefit.

3. Data Limitation

The regional LPR server is not to be accessed for the purpose of monitoring individual activities protected by the First Amendment to the United States Constitution. The regional server does not contain alert lists for any of the following activities: insurance issues, parking scofflaws, deadbeat parents, and/or vehicle impounds.

The LPR system exists for the sole purpose of assisting law enforcement officers with ongoing criminal investigations and only for authorized public safety purposes.

4. Performance Evaluation

In addition to audit reports, ARJIS staff regularly monitors the LPR system for performance, reliability, and functionality. Staff also provides system-generated management reports for the participating agencies that highlight agency use, the number of license plate reads on file, and any technical issues identified during the reporting period. Other system-generated reports are produced on an as-needed basis.

5. Transparency and Notice

ARJIS is a Joint Powers Agency governed by the San Diego Association of Governments (SANDAG) Public Safety Committee, which includes elected officials representing the sub-regions of San Diego County and public safety officials.

LPR systems managed and hosted by individual law enforcement agencies existed within San Diego County prior to implementation of the LPR system. A PIA and Regional LPR Guidelines were completed prior to implementation of the LPR system.

This Acceptable Use Policy, the associated PIA, and other governing documents are currently posted on the ARJIS website at ARJIS.org.

6. Security

Regional LPR data is stored in a segregated server located 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 and select ARJIS technical staff who have completed background investigations and completed the relevant FBI CJIS state and federal training.

Authorized ARJIS technical staff shall have the responsibility for managing the LPR system and associated infrastructure. ARJIS utilizes strong multi-factor authentication, encrypted communications, firewalls, and other system auditing, physical, administrative, and security measures to minimize the risks of unauthorized access to the system.

7. Retention, Access, and Use of LPR Data

7a. Retention

LPR data sent to ARJIS and stored on the regional server will be retained for a period of twelve months. The retention policy is consistent with the policies of the majority of agencies in California that have implemented LPR systems as of January 2015. Once the retention period has expired, the record will be purged from the active database. If an agency determines select LPR data is relevant to a criminal investigation, it is the responsibility of that agency to document and retain those records on its own server in accordance with the agency's policies regarding records retention. In the event California passes pending LPR legislation, this provision will automatically incorporate the retention period mandated in the legislation and will

supersede the 12-month period set forth above.

7b. Requirements for All Users Accessing Regional LPR data

Various measures are taken by ARJIS to limit access to the regional LPR server to prevent unauthorized access. Only those authorized personnel who have met the minimum training, certification, and background checks required for access to criminal justice data may access the regional LPR server. These requirements concerning the security and confidentiality of all 'justice data' are set forth in the FBI CJIS Security Policy and the CLETS PPP.

Authorized users must have an active account in the ARJIS Security Center, are mandated to follow the procedures for establishing complex passwords that must be changed every 90 days, and must enter a reason for access to LPR data prior to executing a query. These requirements are all built into the LPR system and are enforced using data entry fields that users must populate in order to access the regional LPR server. All queries for LPR data are subject to audit and kept in audit logs in accordance with the procedures outlined in the audit section below.

7c. Use of LPR data

LPR data is for official law enforcement purposes only. Participating law enforcement agencies will not share LPR data with commercial or private entities or individuals. However, participating law enforcement agencies may disseminate LPR data to governmental entities with an authorized law enforcement or public safety purpose for access to such data, in accordance with existing FBI and Cal DOJ policies, and their agency's standard operating procedures. ARJIS assumes no responsibility or liability for the acts or omissions of such agencies in disseminating or making use of the LPR data.

8. Auditing and Accountability

ARJIS has developed preset queries to the regional LPR server for auditing and other tracking functions. Included are audit capabilities for individual user activity, management reports of interface functionality and reliability, reports from session logs, and other key system metrics.

Access to, and use of, LPR data is logged for audit purposes. Audit logs are maintained for a minimum of three years. Audit reports are structured in a format that is understandable and useful and will contain, at a minimum:

- The name and agency of the user
- The date and time of access
- The specific data queried

- The justification for the query including a relevant case number if available at the time.

ARJIS will provide specific information regarding individual access and queries upon request from any agency. Identifying and addressing intentional misconduct is the responsibility of the individual agency. Notwithstanding the participating agency's responsibility with regard to misconduct, ARJIS reserves the right to enforce this Policy as described below.

9. Enforcement of Policy

Violation of this Policy by an ARJIS member agency or its staff may lead to suspension or termination of an agency or particular agency staff person's access to the regional LPR system. In the event a member agency discovers suspected or actual misuse of the regional LPR system, it will immediately inform the Director of ARJIS, who will in turn immediately notify the SANDAG Director of Technical Services and SANDAG Executive Director. In the event ARJIS discovers suspected or actual misuse of the regional LPR system, the Director of ARJIS will immediately notify the SANDAG Director of Technical Services, the SANDAG Executive Director, and the agency. The Technical Services Director, in consultation with the Director of ARJIS, or their designees, will determine whether to suspend or terminate access and if so for whom the suspension or termination will apply and will notify the affected agency. The affected agency will be notified of the decision by SANDAG and then will have 10 calendar days to appeal the decision to the SANDAG Executive Director. The Executive Director shall have final decision-making authority.

10. Policy Revisions

The Acceptable Use Policy for the Regional LPR System will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least once per year for review and determination regarding the need for amendments.

Updates regarding the LPR system will be provided to the SANDAG Public Safety and Chiefs'/Sheriff's Management Committees annually or upon request.

11. Indemnification

Each user of the Regional LPR system (User) agrees to indemnify and hold SANDAG and ARJIS, and each of their personnel, harmless from any claim or demand, including reasonable attorneys' fees, made by any third-party in connection with or arising out of User's use of the Regional LPR system, User's violation of any terms or conditions of this Policy, User's violation of applicable laws, regulations or other policies, or User's violation of any rights of another person or entity. The term "Users" is defined to include each agency accessing the LPR system, as well as each individual person with access to the LPR system.