<table>
<tr><td colspan="2"></td><td colspan="4" align="center">SOUTH MIAMI
POLICE DEPARTMENT</td></tr>
</table>

GENERAL ORDER NUMBER: 18-14	DATE OF ISSUE: October 01, 2019	EFFECTIVE DATE: October 01, 2019	NUMBER OF PAGES: 07
CFA STANDARD: 32.04 SUBJECT: Automated License Plate Reader/Recognition System	NEW (XX) RESCINDS ( ) AMENDS ( ) OTHER ( )	By Order Of: Rene Landa, CHIEF OF POLICE	

CFA STANDARDS: 32.04

SECTIONS:

18.14.1

PURPOSE: The purpose of this policy is to establish guidelines for the issuance, training, and use of the Automated License Plate Reader system (A.L.P.R.).

SCOPE: This General Order applies to all departmental personnel.

POLICY: The South Miami Police Department will only use the A.L.P.R. system in support of official law enforcement activities and Homeland Security operations in accordance with local, state, and federal law.

Automated License Plate Reader (A.L.P.R.) technology assists law enforcement in the detection, identification, and recovery of stolen vehicles, wanted persons, missing and/or endangered children/ adults and persons who have committed serious and/ or violent crimes. A.L.P.R. data can assist investigators in developing and pursuing leads in criminal investigations by assisting in locating suspects, witnesses, and victims through vehicle license plate data. As with any technology, specifically the A.L.P.R., it is incumbent upon the user utilizing the system, to put necessary safeguards in place that will instill public confidence that the data and subsequent information will be used appropriately (in accordance with departmental policy and applicable laws).

18.14.2

DEFINITIONS:

A. **ALERT:** An indication by visual and/or audible signal of a potential match between a license plate scanned by the A.L.P.R. system and the data on the Hot Lists.

B. **AUTOMATED LICENSE PLATE READER (A.L.P.R.):** A specialized system consisting of a camera(s), computer and computer software that automatically recognizes the characters on vehicle license plates, compares the data against a list of license plates bearing some significance to law enforcement, and notifies trained users when there is a match. The A.L.P.R. may be mounted to a police vehicle, hand-held, or be stationary/fixed at a location.

C. **A.L.P.R. SYSTEM ADMINISTRATOR**: Designated Uniform Patrol Division Lieutenant.

D. **HISTORICAL A.L.P.R. DATA**: A database containing the dates, times, and locations of individually identifiable vehicle license plates that is stored for a limited period of time and reference.

E. **HIT**: A read matched to a license plate that has previously been registered on an agency's "Hot List" of vehicle license plates related to; stolen vehicles, stolen license plates or other factors supporting investigation, or which have been manually registered by a user for further investigation.

F. **HOT LIST**: A list of license plates and vehicles entered into the National Crime Information Center (NCIC), Florida Crime Information Center (FCIC), and Driver and Vehicle Information databases (DAVID) as well as any information that is entered manually by any participating law enforcement agency.

G. **LOCAL ENTRY**: Entry made by local law enforcement for matters having a legitimate law enforcement and/or Homeland Security purpose requiring immediate dissemination.

H. **OFFICIAL LAW ENFORCEMENT ACTION**: An encounter where a law enforcement officer, acting in an official capacity, takes enforceable action (i.e.: arrests, traffic citation, civil citation, etc.). Although every encounter that may result in an official law enforcement action cannot be identified, officers are to use their training and experience to determe what may turn into an official law enforcement matter.

I. **MCT**: Mobile Computer Terminal.

J. **READ**: Digital images of license plates and vehicles and associated metadata that includes dates, times, and geographical coordinates associated with the vehicle image captured by the A.L.P.R. system.

18.14.3

PROCEDURES; ASSIGNMENT, MANAGEMENT, AND OPERATION:

I. Assignment

A. A.L.P.R. equipment will only be utilized by personnel (users) trained in its use and operation. [CFA 32.04(A)].

B. Individual officers will be responsible for the care and custody of their assigned A.L.P.R. system.

C. The deploying officer will be responsible for the care and custody of the stationary/ fixed (Traffic Trailer) A.L.P.R. system.

II. Management

A. A designated Uniform Patrol Lieutenant or designee will be responsible for the administration, maintenance, and deployment of the A.L.P.R. system.

B. A.L.P.R. users will not attempt to modify A.L.P.R. equipment or software without written authorization from the A.L.P.R. System Administrator.

C. A.L.P.R. camera lenses may be cleaned with glass cleaner or mild soap and a nonabrasive soft cloth.

D. Vehicles with external A.L.P.R. equipment attached will not be cleaned in an automated car washing facility.

E. Damage to A.L.P.R. equipment will be immediately reported to their supervisor and the A.L.P.R. System Administrator (via email). The supervisor will document and investigate the damage in accordance with departmental policies.

III. Operation

A. At the beginning of each A.L.P.R. deployment users will ensure:

1. The A.L.P.R. system has been updated with the most current Hot List available; and

2. The A.L.P.R. system is working properly. Malfunctioning equipment will be reported to the A.L.P.R. System Administrator (via email). The A.L.P.R. System Administrator will ensure the equipment is repaired. The malfunctioning equipment will not be used.

B. A.L.P.R. users will specify when law enforcement action is taken due to the use of the A.L.P.R. on their daily worksheet by the end of their shift or detail.

C. The use of the A.L.P.R. shall be documented on the appropriate official departmental report (i.e., Offense-Incident Report, Field Interview Reports, Uniform Traffic Citations, Arrest Forms, etc.).

D. A.L.P.R. user will verify an Alert prior to conducting a traffic stop. An unverified Alert will not be used as the sole reason for initiating a traffic stop. An A.L.P.R. traffic stop will only be conducted when the Alert is validated, which establishes reasonable suspicion or probable cause. Verification will be made by:

1. Visually confirming the alphanumeric characters and state of issuance of the physical license plate matching the Alert image displayed by the A.L.P.R. system. The Alert will be rejected if the image is not the same as the license plate examined visually; and

2. Verifying the status of the Alert through a live Criminal Justice Information System (CJIS) to include but not limited to; NCIC, FCIC, and DAVID.

E. Supervisors are responsible for monitoring A.L.P.R. users under their command to ensure compliance with department policy and procedures pursuant to this General Order.

18.14.4

CRITERIA FOR ACTIVATION [CFA 32.04(B)]:

A. A.L.P.R. equipment will only be used to support law enforcement activities and Homeland Security operations in accordance with local, state, and federal law. Information relating to criminal or terrorist acts pursuant to an investigation based on A.L.P.R. is shareable.

1. The A.L.P.R. is authorized for, but not limited to, the interdiction of revoked/suspended driver license, recovery of stolen property, enforcement of stay-away-orders, apprehension of individuals pursuant to outstanding arrest

warrants, interdiction of criminal and/or terrorism suspects and license plate data related to stolen license plates, vehicles displaying those stolen license plates, stolen vehicles, wanted persons, license plates associated with AMBER, SILVER, or BLUE ALERTS, license plates that may be associated with previously undetected criminal acts, license plates linked through investigation to criminal suspects for specific criminal acts, license plates that may be associated with unsolved criminal acts, license plates that may associated with selected traffic enforcement and crime analysis [CFA 32.04(B)].

2. The A.L.P.R. system takes a digital photograph of every license plate that enters its "field of view." It then searches a Hot List file located on the LEARN server and compares the scanned license plate against the FCIC/NCIC Hot List or the agency Local Hot List. The A.L.P.R. system does not conduct a live check against NCIC/FCIC.

3. The Vigilant Solution A.L.P.R. LEARN server is a cloud based A.L.P.R. system with a hosted server located in a secure location within the Miami Beach Police Department. The LEARN server automatically downloads a Hot File from the Florida Department of Law Enforcement. The Hot File for FCIC is downloaded every (3) three hours whereas the Hot File for NCIC will be downloaded twice a day.

4. The A.L.P.R. does not identify a specific person. The data collected by the A.L.P.R. is fact-based information, and absent any effort to link data to another source, is not intelligence data. All enforcement action will be consistent with General Order #1.2.9; Bias Based Profiling.

5. The A.L.P.R. is not to be used to capture license plate information on any person or groups in locations that might reflect on a persons or groups political views, religious views, social views, associations or activities unless there is an independent basis to suspect criminal conduct or activity.

6. Manual Hot List entries will be limited to communications personnel only after authorization and approval by the Uniform Patrol Division Supervisor or the Criminal Investigations Division Supervisor.

18.14.5

DATA SHARING AND DISSEMINATION [CFA 32.04(C)]:

A. Collection: A.L.P.R. data will be collected as a by-product of the active scanning of license plates that are compared with the downloaded extract or searched as part of a criminal investigation or in furtherance of a criminal justice purpose. The data is stored in the A.L.P.R. systems database. A.L.P.R. data will be stored, purged, destroyed or deleted in accordance with Florida Statute 316.0777 and 316.0778.

B. Information Sharing: A.L.P.R. data captured and stored may be shared with other Criminal Justice Agencies for the purpose of conducting ongoing or continuing criminal investigations and for the purpose of active criminal intelligence operations through the LEARN server. The sharing of A.L.P.R. data through the LEARN server is authorized by the Chief of Police or his/her designee. [CFA 32.04(C)]

    1. Information sharing among agencies shall be dictated in accordance with any active Memorandum of Understanding (MOU) or established agency policies and procedures.

    2. A.L.P.R. data is for official use only and will be shared only to other agencies for legitimate law enforcement purposes.

18.14.6

ACCESS AND RETENTION [CFA 32.04(D)]:

A. The Vigilant Solution A.L.P.R. system does not perform secondary capture of PII or CJI and does not need to conform to the FBI CJIS Security Policy (CSP). The A.L.P.R. system will provide user level access based on the role of the person accessing the system to ensure the integrity of the system and confidentiality of the data. The A.L.P.R. system shall be sufficiently designed to minimize the compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data. All searches will require the user to enter a case number and criminal justice purpose. [CFA 32.04(D)]

B. The A.L.P.R. Hot List data will be maintained by the FDLE.

C. The A.L.P.R. data will be purged by the vendor after a (1) one year period unless there is a compelling reason to retain the information longer. A.L.P.R. data will be stored, purged, destroyed or deleted in accordance with Florida Statute 316.0777 and 316.0778. With the written approval of the A.L.P.R. System Administrator, a documented request to the vendor will be made for the retention of A.L.P.R. data

longer than the (1) one year period so long as the requested A.L.P.R. data is related to a specific open investigation linked to a specific case number. [CFA 32.04(D)]

D. The A.L.P.R. database will be made available for search by trained department personnel for legitimate, specified, and documented law enforcement purposes. Searches are documented in the database.

E. Active and historical A.L.P.R. data is classified for Official Use Only.

F. The collection and/or dissemination of A.L.P.R. data outside the parameters of this General Order may result in discipline up to, and including termination.

G. Downloading of A.L.P.R. data by an employee to any personal storage device, camera, or other mobile device is prohibited.

18.14.7

TRAINING [CFA 32.04(A)]:

A. The A.L.P.R. System Administrator will be responsible for the development of training and for assuring proficiency of operators with the A.L.P.R. system.

B. Lesson plans will be based on manufacturer recommendations, regulations, and legal mandates governing the use of NCIC/FCIC and DAVID systems and controlling law. Training criteria will be reviewed and revised as needed.

C. Prior to using the A.L.P.R. system, members must be actively certified on FCIC/NCIC and DAVID systems, complete the A.L.P.R. approved course and demonstrate proficiency on the systems capabilities.

D. Training will be conducted and documented (required departmental training forms) by users qualified to instruct.

E. All records of training and attendance will be forwarded to the Training Unit.

F. A list of qualified users will be maintained by the A.L.P.R. System Administrator.