INDIANA STATE POLICE	***STANDARD OPERATING PROCEDURE*** State Form 39870(R/S-06)	Reference Number ENF-017
	Subject License Plate Reader	
	Special Instructions Replaces ENF-017 dated March 1, 2015	Effective Date **August 18, 2023**

I. PURPOSE

Establish operational procedures for the use of the license plate reader (LPR) system and the retention of data. The intended use of the LPR system is to increase public safety, minimize the threat and risk of injury to individuals, to enhance the criminal investigatory process, and make the most effective use of public resources allocated to public safety agencies.

II. POLICY

The ISP utilizes LPR systems comprised of fixed and mobile license plate readers and the associated database(s), which can be used to scan, detect, collect, analyze, and disseminate identified license plate information. License plate numbers and date/time location collected through an LPR system may not be, when taken alone, sufficient to identify the individual associated with the vehicle.

III. DEFINITIONS

A. Agency – A law enforcement agency with access to the LPR system. As used in this policy for hot lists, agency refers to the entirety of an agency, not an individual user of the LPR system within an agency.

B. LPR Coordinator – Special Investigations Division Commander or designee.

C. LPR User – Department employees trained and authorized to utilize LPR.

D. License Plate Reader (LPR) - A device that uses cameras and technology to compare digital images of license plates against databases.

E. Detection – Image capture of a license plate and/or vehicle.

F. Hit – An alert from the LPR system that a scanned license plate number may be in NCIC or another law enforcement database for a reason including, but not limited to, being related to a stolen car, wanted person, missing person, violent crime or terrorist-related activity.

G. Hot List/Hot Plate - A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to, NCIC, IDACS, etc. For the purposes of this SOP, Hot List/Hot Plates will be referred to as Hot List. Hot lists created by ISP employees shall be categorized as:

1. Non-Shared - Only the entering person has access to the Hot List.
2. Group* – The entering individual and other individuals added by the entering individual, who are working on a common detail.
3. Shared - Any Hot List that is accessible to the entire agency and/or other agencies.

*NOTE – A Group Hot List can include individuals of another agency without meeting the Shared Hot List requirements. Shared Hot List requirements apply when the Hot List is being shared fully within the Department or another agency.

H. Individual – a single user of the LPR system. An individual may be an ISP employee or an employee of another agency.

I. Inquiry – A search of the LPR database for specific information.

J. Vehicles of Interest – Vehicles, including but not limited to those which are reported as: stolen; displaying stolen license plates or tags; linked to missing and/or wanted person; linked to violent crimes and/or flagged by law enforcement officers or agencies for an official law enforcement purpose.

IV. PROCEDURE

A. An inquiry into the LPR system requires a legitimate law enforcement purpose and must be documented in a CAD and/or a case report. The report must document the usage, the basis for the inquiry, and the action taken. If a case report is created, "Incident involving LPR" shall be selected.

B. It is a violation of this policy to use the LPR system, associated scanned files or Hot Lists for the purpose of infringing upon First Amendment Rights, including information related to individuals or organizations based solely on their religious, political, social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, age, disability, gender, sexual orientation, or other classification protected by law.

C. Personnel shall not use the LPR system in violation of federal or state laws.

D. Personnel shall not permit any unauthorized use of the LPR system and shall not transfer, provide or otherwise communicate or share an individual username and/or password.

E. Personnel given access to LPR system shall:

1. Be responsible to use and properly maintain the LPR system access.
2. Complete a CAD or case report entry documenting each inquiry (for auditing purposes).

F. LPR Coordinator Duties and Responsibilities:

1. Issue, manage, and/or revoke account access.
2. Audit the LPR system(s).
3. Address issues or concerns directly with vendors.
4. Coordinate outside agency requests for data sharing.
5. Provide training for approved employees and document training in ACADIS.
6. Maintain all LPR related records.

G. DIC Responsibilities:

1. Audit district personnel's use of the LPR system to ensure a CAD and/or case report number is provided on every inquiry.

2. Any additional duties and responsibilities delegated to the DIC by the LPR Coordinator.

H. LPR Hits

1. If an LPR hit is received, the officer shall confirm the validity of the hit prior to taking

enforcement action* by verifying:

a. The vehicle observed corresponds to the description of the vehicle from the hit.
b. If applicable, the license plate observed matches the plate provided in the hit.
c. The hit is active through dispatch or with the officer's Mobile Data Terminal.

*NOTE - An LPR NCIC/IDACS hit alone may not, without verification, establish reasonable suspicion and/or probable cause.

I. Hot Lists

1. Non-shared lists shall comply with the following:

a. May be utilized for any legitimate law enforcement purpose.
b. It is the responsibility of the entering officer to determine when the information is no longer necessary and ensure the entry or hot list is removed.
c. The officer shall initially set an expiration date for seven (7) days or less. Entry must be reviewed at a minimum of every seven (7) days at which time the expiration date may be extended another seven (7) days or less.

2. Group hot lists shall comply with the following:

a. May be utilized for any legitimate law enforcement purpose.
b. It is the responsibility of the entering officer to determine when the information is no longer necessary and ensure the entry/hot list is removed.
c. Additionally, any authorized user of a group hot list, who becomes aware that an entry or hot list is no longer necessary, shall notify the entering officer that the entry or hot list should be removed. If the entering officer is unavailable, any group member that is aware that an entry or hot list is no longer necessary, shall remove the entry or hot list.
d. The entering officer shall initially set an expiration date for seven (7) days or less. Entry must be reviewed at a minimum of every seven (7) days at which time the expiration date may be extended another seven (7) days or less.

3. Shared hot lists shall comply with the following:

a. Shall be created only for active or ongoing cases involving a Level I or II felony, violent crimes against persons, or exigent circumstances.
b. A shared hot list must be approved by the entering officer's immediate supervisor or Post Command prior to entering.
c. It is the responsibility of the entering officer to determine when the information is no longer necessary and immediately remove the entry or hot list.
d. The entering officer shall remove the entry or hot list immediately upon confirmation that it has been entered into NCIC/IDACs.
e. The entering officer shall initially set an expiration date for three (3) days or less and shall include contact information for the entering officer. The entry or hot list must be reviewed at a minimum of every three (3) days at which time the entering officer may extend the expiration date another three (3) days or less.
f. The entering officer's supervisor or Post Command has discretion to how widely the information is shared. It is recommended that sharing be limited to a narrow scope.

J. Retention of LPR system data

1. LPR information is only retained for thirty (30) days before being purged from the system.

2. Investigative information collected from the LPR system shall be promptly captured by the user and placed into the incident management system to avoid relevant information or evidence being purged.

K. This procedure is to be used in conjunction with all relevant Department regulations, rules, policies, and procedures.