ILLINOIS STATE POLICE DIRECTIVE
ENF-051, AUTOMATED LICENSE PLATE READERS (ALPR)/ LAW ENFORCEMENT ARCHIVAL RETRIEVAL NETWORK (LEARN)

RESCINDS:	**REVISED:**
New Directive	04-07-2022 **2022-169**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
	41.3.9

I. POLICY

The Illinois State Police (ISP) shall utilize an Automated License Plate Reader (ALPR) system to provide information and investigative resources to officers. The ISP will establish basic procedural guidelines and responsibilities of personnel accessing ALPR data utilizing the Law Enforcement Archival Retrieval Network (LEARN). The access and use of the ALPR data shall be for law enforcement purposes only and in compliance with all applicable training, laws, and administrative rules.

II. DEFINITIONS

II.A. Alert - A visual and/or auditory notice that is triggered when the ALPR system receives a potential hit on a license plate.

II.B. Automated License Plate Reader (ALPR) - Equipment consisting of cameras, computer, and computer software used to automatically recognize and interpret the characters on vehicle license plates. Digital images captured by the cameras are converted into data which is processed through the ALPR system. (also known as Automated License Plate Recognition).

II.C. Fixed ALPR System - ALPR cameras that are permanently fixed to a structure, such as a pole, a traffic barrier, or a bridge.

II.D. Hit - A read matched to a license plate that has previously been registered on the Department's hot list of vehicle plates or on the local hot list on the ALPR computer that has been added by a user.

II.E. Hot List - License plate numbers of stolen vehicles, wanted subjects, missing persons, AMBER alerts, suspended, revoked, or expired registration, or any other criteria. Hot list information can come from a variety of sources including but not limited to: the National Crime Information Center (NCIC), Law Enforcement Agencies Data System (LEADS), and the Illinois Secretary of State (SOS).

II.F. Law Enforcement Archival Reporting Network (LEARN) – LEARN is Vigilant Solutions' intelligence platform for law enforcement. LEARN will eliminate specific IT requirements within the Department and provide data security. LEARN transforms disparate sets of data into actionable intelligence. Data such as Fixed License Plate Readers (LPR), Mobile LPR, and Vigilant's own network of private LPR data are merged together with analytics and condensed into meaningful and visual intelligence that increases public safety.

II.G. Mobile ALPR System - ALPR cameras that are affixed, either permanently or temporarily, to a law enforcement vehicle for mobile deployment.

II.H. Motor Carrier Safety ALPR System – ALPR system leased by the Illinois Department of Transportation (IDOT) and operated by Commercial Vehicle Enforcement Officers (CVEO). This system shall contain only federal Department of Transportation (DOT) and Illinois Commerce Commission (ICC) data related to motor carrier safety.

II.I. Portable ALPR System - ALPR cameras that are transportable and can be moved and deployed in a variety of venues as needed.

II.J. Read - The capture of digital images or license plates and vehicles with associated metadata (date, time, GPS coordinates with vehicle image capture).

III. RESPONSIBILITIES

III.A. The Deputy Director of the Division of Patrol (DOP) will designate an ALPR/LEARN System Statewide Coordinator.

III.B. ALPR/LEARN System Statewide Coordinator

III.B.1. The Statewide ALPR/LEARN Coordinator will be the primary point of contact for Millennium/Vetted Solutions and Motorola to establish law enforcement data sharing agreements and future project expansion.

III.B.2. The ALPR/LEARN System Statewide Coordinator will be responsible for ensuring maintenance, and product warranties are upheld pursuant to executed contracts, including five years of licensing for:

III.B.2.a. Commercial LPR Data (unlimited users, unlimited inquiries),
III.B.2.b. Hosting services, OCR updates, Help Desk, and Warranty, and
III.B.2.c. Remote Monitoring Software (based on the number of sensors).

III.B.3. The ALPR/LEARN System Statewide Coordinator is designated as the Agency Coordinator to act as a central point of contact for all FBI-CJIS Security Policy-related matters and assign staff familiar with the contents of the FBI-CJIS Security Policy. The ALPR/LEARN System Statewide Coordinator will:

III.B.3.a. Provide timely updates with specific information regarding any new FBI-CJIS, state, or local information security policy requirements which may impact Vigilant compliance or system/application development and facilitate obtaining certifications, training, and fingerprint-based background checks, as required.
III.B.3.b. Inform Vigilant of any required FBI-CJIS Security Awareness Training, personnel background screenings, or executions of FBI-CJIS Security Addendum Certifications.
III.B.3.c. Inform Vigilant of any relevant data breach or cyber incidents, including DDoS, Malware, Virus, etc., which may impact or harm Vigilant systems, operations, business partners, and/or other Agencies for proper analysis to be performed, and Incident Response Procedures initiated.
III.B.3.d. Be responsible for the legality and compliance of information recorded, submitted or placed in Vigilant systems and use of that data.
III.B.3.e. Be responsible for proper equipment operation and placement of equipment.
III.B.3.f. Vet authorized user access to Vigilant systems with due consideration to providing potential access to non-Agency information.
III.B.3.g. Act as the authority within ISP to grant access to purchased Vigilant systems as well as the data stored and transmitted via Vigilant systems.
III.B.3.h. Ensure all data security, handling, and data protection strategies from point of acquisition, during transport, and through submission (“Hot list upload”) into Vigilant systems.
III.B.3.i. Establish policies and procedures for secure storage and protection of Vigilant system passwords.
III.B.3.j. Develop protocols for creating user accounts with only government domain email addresses. Any exceptions shall be granted in writing.
III.B.3.k. Develop protocols that prohibit the sharing of user accounts.
III.B.3.l. Ensure Vigilant role-based access as designed to foster system security and integrity.
III.B.3.m. Ensure appropriate use and data storage policies and procedures for data maintained outside the Vigilant systems, including any information disseminated, extracted, or exported out of Vigilant systems.
III.B.3.n. Develop and enforce protocols relating to deletion/purging and dissemination of information within and outside the Vigilant systems.
III.B.3.o. Ensure data and system protection strategies are accomplished through the tools provided by Vigilant for account and user management features along with audit and alert threshold features.

III.B.3.p. Ensure "virtual escorting" security tools are provided and used as intended for managing ISP system remote access and will monitor Vigilant support staff when authorized to assist the ISP.

III.B.3.q. Ensure Vigilant designed technical controls and tools are effective in conjunction with ISP policies and procedures that guide user access and appropriate use of the system.

III.B.3.r. Ensure the information and services provided through Vigilant products do not provide any actionable information. Agency users are responsible for the validity and accuracy of their data and developing procedures to verify information with the record owner and other systems (e.g. NCIC) based upon the potential lead generated.

III.C. ALPR/LEARN System Work Unit Coordinator

III.C.1. The Commander of each District, Zone, and/or Specialty Unit seeking to use the ALPR/LEARN System will appoint an ALPR/LEARN System Work Unit Coordinator.

III.C.2. The ALPR/LEARN System Work Unit Coordinator will:

III.C.2.a. Have greater than user access to the LEARN system.

III.C.2.b. Ensure user information is properly entered into the LEARN system.

III.C.2.c. Ensure personnel complete required training prior to using the ALPR/LEARN System.

III.C.2.d. Ensure personnel utilize the system for authorized law enforcement purposes only.

III.D. ALPR/LEARN System Users will:

III.D.1. Attend and complete the Motorola Vigilant and/or Agency training program prior to operating the ALPR/LEARN System.

III.D.2. Utilize the ALPR/LEARN System following the procedures identified in the ALPR/LEARN training program, this Directive, and any other related ISP directives, policies, and procedures.

III.D.3. Only use the ALPR/LEARN System for legitimate law enforcement purposes.

III.D.4. Verify any ALPR/LEARN System hits via LEADS/NCIC before any enforcement action is taken.

III.D.5. Upload any ALPR scan used as evidence into the appropriate report writing platform and digital evidence storage platform consistent with ISP policies and procedures for evidence handling.

III.D.6. Follow guidelines for password protection as outlined in ISP Directive SRV-218, "Computer Password Control."

III.E. The CVEO Section Supervisor shall be responsible for the use of the Motor Carrier Safety ALPR system, and shall:

III.E.1. Approve the deployment of Motor Carrier Safety ALPR systems, including mobile and/or portable systems, and maintain records of usage;

III.E.2. Ensure the system is being used in accordance with the agreement between IDOT and the lessor;

III.E.3. Establish guidelines for usage;

III.E.4. Ensure CVEO personnel operating the system receive training prior to usage;

III.E.5. Ensure data is secure and access is protected.

IV. PROCEDURES

IV.A. ALPR System Limitations for Use

IV.A.1. Use of the ALPR system, software, associated databases, and data is restricted to law enforcement and public safety-related functions. Information obtained from the ALPR, software, associated databases, and data shall not be used for reasons inconsistent with the law enforcement and public safety-related functions under any circumstances.

IV.A.2. Misuse or abuse of the ALPR system, software, associated databases, or data may be subject to sanctions and/or disciplinary action.

IV.A.3. The ALPR system, software, associated databases and data are solely the property of the Department and intended for use in the law enforcement and public safety functions of the Department.

IV.A.4. All ALPR operators must have Law Enforcement Agencies Data System (LEADS) certification prior to operating ALPR equipment or accessing ALPR data.

IV.A.5. Any and all current or future ALPR search software or platforms are subject to authorized user requirements and limitations within this directive.

IV.B. ALPR System Data Confidentiality

IV.B.1. Information obtained from the ALPR system, software, associated databases, and data shall not be disseminated to the public except as authorized or required by law.

IV.B.2. Information obtained from the ALPR system, software, associated databases, and data may be disseminated to other law enforcement agencies or officers only to be used for law enforcement or public safety functions.

IV.B.3. The ISP may share ALPR data with any government entity that presents an authorized law enforcement or public safety purpose. The ISP assumes no responsibility or liability for the acts or omissions of other agencies.

IV.C. ALPR/LEARN System Usage

IV.C.1. The ALPR/LEARN System functions to capture an image of a vehicle's license plate, transform that image into alphanumeric characters, compare the plate to one or more lists of vehicles of interest, and alert the member when a license plate of interest has been observed.

IV.C.2. The ALPR/LEARN System identifies license plates, not vehicles or persons.

IV.C.3. Designated personnel will have the ability to query ALPR/LEARN System data, create reports, and use analytic tools, such as mapping capabilities and compare LPR data with other data sets to enhance law enforcement investigations.

IV.C.4. ALPR/LEARN System cameras are fixed. ISP Personnel will not move or adjust ALPR/LEARN System cameras.

IV.C.5. While conducting a "plate search," users are prompted for a "case number"; for ALPR searches, case numbers include CAD Numbers, Field Report Numbers, Tracs Numbers, I-Case Numbers, Crash Report Numbers, LEADS/NCIC Numbers, and/or outside agency case numbers.

IV.C.6. While conducting a "plate search," users are prompted to enter an "Authorized Purpose." Users are required to enter the criminal nexus authorizing the search (i.e. "expressway shooting," "homicide investigation," "CRIMPAT Detail").

IV.D. ALPR/LEARN System Alerts

IV.D.1. Personnel are encouraged to set LEARN system specifications to receive ALPR alerts.

IV.D.2. Personnel registered to receive ALPR/LEARN System alerts will, at a minimum, receive alerts for felony vehicles, stolen vehicles, AMBER alerts, and SILVER alerts.

IV.D.3. Telecommunication centers will have a system in place to receive ALPR/LEARN System alerts. Telecommunication centers will broadcast alerts received to the appropriate patrol assets.

IV.D.4. Personnel will verify any ALPR/LEARN System hits before any enforcement action is taken.

IV.E. ALPR/LEARN System Record Retention

IV.E.1. ALPR reads will be maintained within the LEARN storage platform for 90 days.

IV.E.1.a. The purging of data after 90 days is a functionality within LEARN and is controlled via system settings.
IV.E.1.b. The ISP System Administrator controls system-wide settings.

IV.E.2. Plate search and plate hit/alert records are maintained permanently within the LEARN storage platform.

IV.E.3. The ISP ALPR/LEARN System Statewide Coordinator will ensure compliance with Illinois Secretary of State Records Retention schedules and procedures.

IV.F. ALPR/LEARN System Technical Support

IV.F.1. All requests for post-installation support will be requested by the ALPR/LEARN System Statewide or Work Unit Coordinators.

IV.F.2. Tier 1 support will be provided by Vetted Solutions.

IV.F.2.a. ISP issues will be submitted to ispsupport@vettedsecuritysolutions.com.
IV.F.2.b. Coordinators may call 727-440-3245 (Help Desk) and select Option 1 to report an issue.
IV.F.2.c. Coordinators may also submit a support ticket directly online by following the steps below:

IV.F.2.c.1) Go to the Vetted Solutions website at www.vettedsecuritysolutions.com.
IV.F.2.c.2) Click the Support Tab on the website's main page.
IV.F.2.c.3) Click the 24/7/Support Helpdesk icon.
IV.F.2.c.4) Choose LPR Tech Support, License Key Request, CCTV and Surveillance Work Etc.
IV.F.2.c.5) Follow the prompts for filling out the details of the issues being experienced.

-End of Directive-