

	WOODBIDGE TOWNSHIP POLICE DEPARTMENT Policy & Procedures AUTOMATED LICENSE PLATE RECOGNITION (ALPR)		
	Chapter: 766	Volume Seven: Traffic Operations	
Date(s):	Authority	General Order #:	File #:
Effective: 7-20-11	Director R. Hubner	11-003	766-111
Revised: 01-29-16	Director R. Hubner	11-003	766-161
Revised: 12-5-22	Director R. Hubner	11-003	766-221
Revised: 4-28-23	Director R. Hubner	11-003	766-231
Revised: 7-18-24	Director R. Hubner	11-003	766-241
Revised:			
LEGAL REFERENCES: New Jersey Attorney General Directive 2022-12			
ACCREDITATION STANDARDS REFERENCES: 41.3.9			

766.1 POLICY & PURPOSE:

766.1.1

POLICY: It is the policy of the Woodbridge Township Police Department to utilize Automatic License Plate Recognition (ALPR) technology to the extent possible in accordance with New Jersey General's Directive 2022-12.

766.1.2

PURPOSE: The purpose of this policy is to establish a uniform policy and procedure for the use of Automated License Plate Recognition technology (ALPR) and Stored ALPR Data.

766.1.3

DEFINITIONS: For the purpose of this policy, the following definitions apply:

- A. **AUTOMATED LICENSE PLATE RECOGNITION (ALPR):** Automated license plate recognition or ALPR is technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. ALPR devices may be placed at a stationary location (permanent or portable) or be mobile and affixed to a police vehicle. The vehicle location data captured by an ALPR device is:
 1. Used to alert law enforcement to vehicles they have a legitimate and specific reason to locate.
 2. Stored so that law enforcement may perform searches to further subsequent investigations. Both situations are described in more detail in this policy
- B. **BOLO (Be on the Lookout):** Refers to a determination by a law enforcement agency that there is a legitimate and specific law enforcement reason to identify or locate a particular vehicle.
- C. **BOLO LIST:** Sometimes referred to colloquially as a "hot list," is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists that is programmed into an ALPR so that the device will alert if it captures the image of a license plate that matches a license plate included on the BOLO list. The term also includes a compilation of one or more

- license plates, or partial license plates, that is compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data that is stored in a separate data storage device or system.
- D. **STORED DATA:** Refers to all information captured by an ALPR and stored in the device's memory or in a separate data storage device or system. The term includes the recorded image of a scanned license plate and optical character recognition data, a contextual photo (i. e.; a photo of the scanned vehicle and/or occupants), global positioning system("GPS") data (when the ALPR is equipped with a GPS receiver) or other location information, and the date and time of the scan. The term applies to both alert data and non-alert data that has been captured and stored by an ALPR or in a separate data storage device or system.
- E. **ALERT DATA:** Means information captured by an ALPR relating to a license plate that matches the license plate on a BOLO list.
- F. **IMMEDIATE ALERT:** Refers to an alert that occurs when a scanned license plate matches the license plate on a BOLO list and that is reported to the officer operating the ALPR, by means of an audible alarm or by any other means, at or about the time that the subject vehicle was encountered by the ALPR and its license plate was scanned by the ALPR.
- G. **NON ENCOUNTER ALERT:** Refers to an immediate alert where the officer operating the ALPR is instructed to notify the agency that put out the BOLO without initiating an investigative detention of the subject vehicle or otherwise revealing to the occupant(s) of that vehicle that its location has been detected or that it is the subject of law enforcement attention.
- H. **PERSONAL IDENTIFYING INFORMATION:** Means information that identifies one or more specific individuals, including an individual's name, address, social security number, vehicle operator's license number, or biometric records. The term includes personal identifying information that is included within the data comprising a BOLO list, as well as personal identifying information that is learned by checking a license plate scanned by an ALPR against the Motor Vehicle Commission database or any other data system that contains personal identifying information.
- I. **SCAN:** Refers to the process by which an ALPR automatically focuses on, photographs, and converts to digital text the license plate of a vehicle that comes within range of the ALPR.
- J. **CRIME SCENE QUERY:** Refers to the process of accessing and reviewing stored ALPR data that had been originally scanned at or about the time and in the vicinity of a reported criminal event for the purpose of identifying vehicles or persons that might be associated with that specific criminal event as suspects, witnesses, or victims.
- K. **CRIMINAL EVENT:** means a specific incident, or series of related specific incidents, that would constitute an indictable crime under the laws of the State of New Jersey, whether or not the incident(s) have occurred or will occur within the State of New Jersey. The term includes an attempt or conspiracy to commit a crime, or actions taken in preparation for the commission of the crime, such as conducting a surveillance of the location to identify and evade or thwart security measures, or conducting a rehearsal of a planned crime. The term includes two or more separate criminal acts or episodes that are linked by common participants or that are reasonably believed to have been undertaken by a criminal organization or as part of an ongoing conspiracy.
- L. **CRIME TREND ANALYSIS:** Refers to the analytical process by which stored ALPR data is used, whether alone or in conjunction with other sources of information, to detect crime patterns by studying and linking common elements of recurring crimes; to predict when and where future crimes may occur; and to link specific vehicles to potential criminal or terrorist activities.

766.2

ADMINISTRATION AND OVERSIGHT:

766.2.1

ADMINISTRATION AND OVERSIGHT OF THE ALPR PROGRAM: The Police Director shall designate an Agency ALPR Coordinator to oversee and administer the department's ALPR program.

766.2.1

AGENCY ALPR COORDINATOR RESPONSIBILITIES: The Agency ALPR coordinator shall:

- A. Be the external point of contact for agency ALPR-related items such as information sharing and audits.
- B. Internally oversee the agency's ALPR program, including training and approving access requests.
- C. Designate authorized users within the agency who can use ALPR's and access stored data. All users must complete all mandated training.

766.2.2

AUTHORIZED USERS: Only sworn or civilian employees who have been authorized by the Police Director and have received training on the proper operation and use of an ALPR and related equipment, and on the provisions of this department's ALPR policy and Attorney General Guidelines may operate an ALPR or access ALPR stored data.

- A. All authorized users are responsible for inspecting any issued ALPR and/or related equipment for any obvious signs of damage or malfunction on an ongoing basis.
- B. Any sworn or civilian employees who discovers a possible problem with an ALPR or related equipment is to notify their supervisor immediately. The supervisor will check for replacement equipment.

766.3 DEPLOYMENT:

766.3.1

DEPLOYMENT OF ALPR'S: ALPR and the data that are collected by these devices stored for future use shall only be used in accordance with Attorney General Directive 2022-12, the manufacturer user's manual, and this policy.

- A. An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business. This also applies to any ALPR data that is collected by another law enforcement agency and provided to this agency or collected by this agency and provided to another law enforcement agency.
- B. An ALPR reader shall only be used to scan license plates of vehicles that are exposed to public view (e.g., vehicles on a public road or street or that are on private property, but which license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shopping mall or other business establishment).

766.3.2

SHARING DEPLOYMENT INFORMATION: The following data must be shared with the State ALPR Coordinator prior to installing or relocating a permanent fixed ALPR unit:

- A. Camera name (pursuant to convention specified by State ALPR Coordinator).
- B. Location (latitude and longitude).
- C. Survey provided by ALPR vendor, including projected size of ALPR data.
- D. When deploying or relocating a portable fixed ALPR unit, the updated latitude and longitude data must be provided to the State ALPR Coordinator.

766.3.3

DECONFLICTION: The ALPR Coordinator shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.

766.4 BOLO LISTS:

766.4.1

STANDARD FOR INCLUDING LICENSE PLATE IN BOLO LIST: A license plate number may be included in a "be on the lookout" or BOLO list (a compilation of license plates or partial plates for which a BOLO situation exists) for input into an ALPR system only if there is a legitimate and specific law enforcement

reason to identify or locate that particular vehicle, or any person(s) who are reasonably believed to be associated with that vehicle. Examples of legitimate and specific reasons include but are not limited to:

- A. Persons who are subject to an outstanding arrest warrant.
- B. Missing persons.
- C. AMBER/SILVER alerts.
- D. Vehicles and/or persons involved in prior suspicious activity, such as groups of vehicles travelling together suspected of criminal activity, or subjects trying to open doors to random cars.
- E. Stolen vehicles.
- F. Vehicles reasonably believed to be involved in the commission of a crime or disorderly persons offense.
- G. Vehicles registered to or reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list.
- H. Vehicles with expired registrations or other Title 39 violations.
- I. Persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements.
- J. Persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity.
- K. Persons who are on any watch list issued by a state or federal agency responsible for homeland security.

766.4.2:

BATCH DOWNLOADING: BOLO list information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, US Department of Homeland Security, and Motor Vehicle Commission database.

766.4.3:

UPDATING BOLO LISTS: A BOLO list may be revised at any time. Updates to a BOLO list shall be done at the start of each shift for mobile ALPRs attached to police vehicles, and as frequently as possible, but at least daily, for ALPRs at stationary locations.

766.4.4

IMMEDIATE ALERT RESPONSE: A BOLO match with an ALPR scan may be programmed to trigger an immediate alert. The reason for including the vehicle on the BOLO list shall be disclosed to the officer who will react to an immediate alert. The officer should determine whether the alert has been designated as a non-encounter alert (meaning officer should not encounter the vehicle) and, if so, follow any instructions included in the alert for notifying the originating agency.

- A. When an officer receives an immediate alert without a non-encounter restriction, the officer shall take such action in response to the alert as is appropriate in the circumstances. An officer alerted that an observed motor vehicle's license plate is on the BOLO list may be required to make a reasonable effort to confirm that a wanted person is actually in the vehicle before the officer would have a lawful basis to stop the vehicle. See *State v. Parks*, 288 N.J. Super. 407 (App. Div. 1996) (no reasonable suspicion to justify a stop because registered car owner's license suspended unless driver generally matches the owner's physical description (e.g., age and gender)).

766.5

ACCESSING STORED DATA:

766.5.1

ALERT DATA: An authorized user may access and use stored ALPR alert data (i.e., ALPR license plate data matching an entry on a BOLO list) as part of an active investigation or for any other legitimate law enforcement purpose, including but not limited to a BOLO query, a crime scene query, or crime trend analysis (as defined in Section 766.5.2 C).

766.5.2

NON-ALERT DATA: Access to and use of stored non-alert ALPR data (i.e., ALPR data gathered not matching a BOLO list entry) is limited to the following three purposes explained below: a BOLO query, a crime-scene query, and crime trend analysis (system tests and troubleshooting are also acceptable purposes).

- A. **BOLO QUERY:** Agencies may compare a BOLO list against stored non-alert data where the results of the query might reasonably lead to the discovery of evidence or information relevant to any active investigation or ongoing law enforcement operation or where the subject vehicle might subsequently be placed on an active BOLO list (for example, may review data to determine whether a specific vehicle was present at the time and place where the ALPR data was initially scanned to check an alibi defense or to develop lead information for the purpose of locating a specified vehicle or person; or to determine whether a vehicle that was only recently added to a BOLO list had been previously observed in the jurisdiction before being placed on the list).
- B. **CRIME SCENE QUERY:** Agencies may access and use stored non-alert data where such access might reasonably lead to the discovery of evidence or information relevant to the investigation of a specific criminal event (i.e., incident that would constitute an indictable crime under New Jersey law). Such queries may not be conducted to review data based on general crime patterns (e.g., to identify persons traveling in or around a “high crime area”). A record shall be kept of the specific crime(s) justifying the query, including the crime date and location.
- C. **CRIME TREND ANALYSIS:** Agencies may access and use stored non-alert data where such access, which may be automated, might reasonably lead to the discovery of evidence or information relevant to an investigation that is not related to a specific criminal event. Such access must be approved by the Agency ALPR Coordinator or their designee.
 - 1. Crime trend analysis shall not result in the disclosure of personal identifying information (such as name, address, SSN, vehicle operator’s license number) to an authorized user or any other person unless:
 - a. There exist “specific and articulable facts that warrant further investigation” of possible criminal or terrorist activity by the driver or occupants of a specific vehicle and access has been approved by a designated supervisor.
 - b. Disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena.
 - 2. Any crime trend analysis shall document:
 - a. The nature and purpose of the crime trend analysis.
 - a. The authorized users who accessed stored non-alert data.
 - b. The designated supervisor who approved access .
 - c. Where personal identifying information was disclosed, (a) the specific and articulable facts that warrant further investigation and (b) the designated supervisor who approved the disclosure of personal identifying information; or, where applicable, the fact that a grand jury subpoena authorized access to personal identifying information.

766.6**SHARING DATA:****766.6.1**

STATEWIDE API: The State ALPR Coordinator shall implement a “Statewide API” (application program interface) that allows access to stored ALPR data across agencies, and specify the method by which all ALPRs used by New Jersey agencies must provide real-time access to ALPR data through the API. Agencies may also share data regionally with other New Jersey agencies pursuant to the mandates of this Directive, and ALPR data collected by a private entity that has entered into an agreement with New Jersey law enforcement can be shared with New Jersey agencies. All ALPRs must make data available to the Statewide API by the effective date of this Directive, and subsequent ALPRs must do so within 45 days of deployment. ALPR systems must be programmed to capture data parameters and meet minimum requirements for accuracy and performance as specified by the State ALPR Coordinator.

766.6.2

SHARING WITH AGENCIES NOT COVERED BY AG DIRECTIVE 2022-12: An agency may enter into a written agreement to share ALPR data with, or receive data from, a law enforcement agency outside of New Jersey or otherwise not covered by this Directive with the approval of the State ALPR Coordinator. Only federally recognized law enforcement agencies may receive access to a New Jersey agency's ALPR data. The State ALPR Coordinator may agree to share ALPR data with a law enforcement agency outside of New Jersey if the out of state agency agrees in writing to use the data only for documented, legitimate law enforcement purposes and to follow other restrictions required by the State ALPR Coordinator in order to achieve the objectives of this Directive. Private entities may provide ALPR data to New Jersey agencies but cannot receive law enforcement-owned ALPR data.

766.7**STORAGE, RECORDS AND RETENTION:****766.7.1**

STORAGE OF ALPR DATA: All ALPR data shall be stored securely and maintained electronically with access restricted to authorized users. ALPR data shall be the property of the agency and not any ALPR vendor. Agencies may jointly store their ALPR data. Commercially obtained ALPR data shall not be co-mingled with law enforcement data. Data being used in an investigatory process shall be maintained in accordance with the agency's evidence or records management procedures.

766.7.2

DEPLOYMENT RECORDS: The following information regarding each ALPR owned or operated by this department shall be maintained:

- A. Date and time deployed.
- B. Portable or fixed.
- C. Identity of operator.
- D. Vendor name.
- E. Date ALPR data connected to Statewide API .

766.7.3

STORED ALPR DATA ACCESS RECORDS: This department shall maintain an automated record-keeping of all access to stored ALPR data including the following:

- A. Date and time of access, and for non-alert data, the justification for access.
- B. Authorized accessor name.
- C. Whether an automated software program was used to analyze the data.
- D. Designated supervisor who approved disclosure of personal identifying information based upon crime trend analysis.
- E. Instances of testing or troubleshooting an ALPR system .
- F. Any other information required to be documented under this Directive.

766.7.4

RETENTION: Records and ALPR data covered by this Section shall be retained for three years.

- A. ALPR stored data shall be purged after the retention period, unless it is associated with an active investigation or pending judicial process, in which case the data should be exported from the relevant storage system and retained in the case file.
- B. Any ALPR data transferred to another agency shall indicate the date on which the data had been collected by the ALPR so that the receiving agency may comply with required retention and purging period.
- C. Records shall be kept in a manner that makes them readily accessible for audit.

766.8 DISCOVERY:

766.8.1

CRIMINAL INVESTIGATORY RECORDS: Stored ALPR data shall be treated as “criminal investigatory records” within the meaning of N.J.S.A. 47:1A-1 et seq., and shall not be shared with or provided to any person, entity, or government agency other than a law enforcement agency, unless a subpoena or court order authorizes such disclosure or unless such disclosure is required by court rules governing discovery in criminal matters.

- A. Any agency receiving a subpoena or court order for the disclosure of ALPR data shall, before complying with the subpoena or court order, provide notice to the County Prosecutor (or Director of the Division of Criminal Justice (DCJ)).

766.8.2

RELEASE OF ALPR DATA: If ALPR data is accessed as part of an investigation—including but not limited to a BOLO query, a crime scene query, or crime trend analysis—a record of the access, which may be automated, and corresponding data shall be included in the agency’s investigative file (electronic or physical). If the investigation results in criminal charges, the ALPR records shall be turned over in discovery pursuant to applicable court rules and case law.

766.9 VIOLATIONS, AUDITS AND TRAINING:

766.9.1

VIOLATIONS: Any knowing violation of this Directive or related agency standing operating procedure, directive, or order, or applicable law, shall be subject to discipline.

- A. All significant violations of the Attorney General Directive or agency policy, including but not limited to unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor (or DCJ Director) and County and State ALPR Coordinator upon discovery. Unless the County Prosecutor or Director elects to conduct or oversee the investigation of the violation, such notification of the violation shall be followed up with a report, approved by the law enforcement executive and with notification to the State ALPR Coordinator, explaining to the County Prosecutor or to the Director, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.
- B. Any complaints about an agency’s ALPR program made by any citizen or entity shall be forwarded to the appropriate County Prosecutor (or DCJ Director), for appropriate review and handling, as well as notification to the County and State ALPR Coordinator. The County Prosecutor or Director may conduct an investigation or direct the agency that is the subject of the complaint to conduct an investigation and report back to the County Prosecutor or Director, with notification to the State ALPR Coordinator.
- C. If the Attorney General or their designee has reason to believe that a law enforcement agency is not complying with or adequately enforcing the provisions of this Directive, the Attorney General may temporarily or permanently suspend or revoke the authority of the department, or any officer or civilian employee, to operate an ALPR, or to gain access to or use ALPR stored data. The Attorney General or designee may initiate disciplinary proceedings and may take such other actions as the Attorney General, in their sole discretion, deems appropriate to ensure compliance with this Directive.

766.9.2

AUDITS: By January 31 each year, the Agency ALPR Coordinator shall perform an audit of their agency’s ALPR program and provide it to the County and State ALPR Coordinator. The County ALPR Coordinator or State ALPR Coordinator may also conduct an audit of the ALPR program at any time.. The audit shall certify the following:

- A. Agency has an ALPR policy in place .

- B. Only authorized users have accessed ALPR data.
- C. Date of each authorized user's last ALPR training .
- D. That a random survey of ALPR accesses revealed no misuse.
- E. A description of any known significant violations and citizen complaints and whether they have been forwarded to the County Prosecutor or DCJ Director.

766.9**VIOLATIONS, AUDITS AND TRAINING:**

- A. INITIAL TRAINING: The State ALPR Coordinator shall design and disseminate training on ALPR technology, including the application of this directive and privacy and security considerations. Completing this required training is a prerequisite for an individual being designated an authorized user under this policy. All ALPR training shall be documented.
- B. REFRESHER TRAINING: Authorized users must complete refresher trainings every two years, as determined by the State ALPR Coordinator. All training shall be documented.

766.10**AGENCY AND VENDOR REQUIREMENTS:****766.10.1**

PROCEDURES: The New Jersey Statewide Networked ALPR Program (NJ SNAP) has been authorized to provide the Hotlists (NCIC and MVC) and NJ SNAP Points of Interest (POI) directly to ALPR vendors. All vendor personnel who have unescorted access to CJI must:

- A. Complete CJIS Security Awareness Training and sign the Information Technology Security Awareness Training Acknowledgment (NJSP S.P. 057 Form, Annex A) bi-annually and provide the form to the department ALPR coordinator.
- B. Sign the Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum Certification (Form H8, Annex B) for the Criminal Justice Information Services (CJIS) Security Policy annually and provide the form to the department ALPR coordinator.
- C. Conduct a national fingerprinting-based record check.
- D. The Department ALPR Coordinator must collect the Information Technology Security Awareness Training Acknowledgment (NJSP S.P. 057 Form) biannually, collect Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum Certification (Form H8) annually, and ensure a national fingerprinting based-record check was completed for all vendor personnel.
- E. The Department ALPR Coordinator will complete an application for the License Plate Reader (LPR) Program for access to NCIC and MVC Hotlist when requested by NJ SNAP.

766.10.2:

VENDOR FUNCTIONS: Any vendor personnel, meeting the CJI requirements listed above, can conduct any authorized administrative or operational ALPR function by request of a LE agency. Vendor personnel access is subject to audit. In addition, vendors must provide NJ SNAP with a list of all LE agencies they intend to provide the Hotlists. NJ SNAP will contact this department and confirm the access request. An application for access to NCIC and MVC hotlist (Application for the License Plate Reader (LPR) Program) must be completed by the Department ALPR Coordinator. NJSP CJIS Control Unit (NJSP CJISCU) will review the CJIS compliance of the LE agency and NJ SNAP will provide written notification of Hotlist access approval or denial to the Vendor. No connection can be made, or Hotlist provided to an LE agency without NJ SNAP approval.