BLOOMFIELD POLICE DEPARTMENT
GENERAL ORDERS

VOLUME: 5	**CHAPTER: 12**	**# OF PAGES: 21**

SUBJECT: AUTOMATED LICENSE PLATE READERS

BY THE ORDER OF: **Chief of Police**	**ACCREDITATION STANDARDS: N/A**
Effective Date:	**SUPERSEDES ORDER #:** **V5C12 (10/21/2014) Rev: (02/27/2023), 06/04/2024**

PURPOSE The purpose of this general order is to maintain direction for agency personnel on the appropriate use of automated license plate readers (ALPRs) and the data that are collected and stored by these devices. This general order is not intended to serve as a comprehensive operational manual. Rather, it is meant to ensure that ALPRs and ALPR-generated data are used in an appropriate manner and only for bona fide public safety purposes.

POLICY It is the policy of the Bloomfield Police Department to utilize ALPR technology to the extent possible in accordance with Essex County Prosecutor's Office directives and *New Jersey Attorney General's Directive 2022-12.*

PROCEDURES

I. DEFINITIONS

1. Agency ALPR Coordinator – is the main point of contact within a law enforcement or public safety agency or authority, designated by the Chief of Police who will be the external point of contact for agency ALPR-related items such as information sharing and audits; internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors); and designate authorized users within the agency who can use ALPRs and access stored data.

2. Alert Data – means information captured by an ALPR relating to a license plate that matches the license plate on a BOLO list.

3. Automated License Plate Recognition (ALPRs) – is technology that uses optical character recognition on images to read vehicle registration plates to create vehicle location data. ALPR can be a system consisting of a camera, or cameras, and related equipment that automatically and without direct human control locates, focuses on, and photographs license plates and vehicles that come into range of the device, that automatically converts digital photographic images of scanned license plates into electronic text documents, that is capable of comparing scanned license plate text data with data files for vehicles on a BOLO (be on the lookout) list that notifies law enforcement, whether by an audible alert or by other means when a scanned license plate matches the license plate on the BOLO list. The term includes both devices that are placed at a stationary location (whether permanently mounted or portable devices positioned at a stationary location) and mobile devices affixed to a law enforcement vehicle and capable of operating while the vehicle is in motion.

4. ALPR Camera(s) – refers to, but is not limited to, high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, handheld devices, or attached to agency vehicles.

5. ALPR System – refers to any software platform or ALPR device (portable or fixed) which connects to a data repository.

6. ALPR Vendor – refers to any business or company providing ALPR solutions or technology systems including, but not limited to, cameras, hardware, software, maintenance, license, data storage, and associated equipment.

7. Authorized User – a sworn or civilian employee who has successfully completed ALPR training designed and disseminated by the State ALPR Coordinator and any training on ALPR policy provided by their agency and has been authorized to operate an ALPR or to access and use ALPR stored data. Employees of a law enforcement agency, public safety agency, or Attorney General's or county prosecutor's office can be authorized users. Authorization shall be given by the agency ALPR Coordinator for each respective agency.

8. 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, or any person(s) who are reasonably believed to be associated with that vehicle.

9. BOLO list – sometimes referred to colloquially as a 'hotlist', is a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists. The list is automatically imported into the vehicle's electronic memory or processor on a regular basis, updated at a minimum every 24-hours, or as appropriate to have the latest information. 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 are compared against stored license plate data that had previously been scanned and collected by an ALPR, including scanned license plate data stored in a separate data storage device or system.

10. BOLO query – refers to the process of querying and comparing a BOLO list against stored non- alert data.

11. Chief – of a law enforcement agency means the highest-ranking executive or sworn officer or officer-in-charge of a law enforcement agency.

12. Commercial ALPR Data – refers to data collected by an entity for commercial purposes.

13. County ALPR Coordinator – is the main point of contact within a county prosecutor's office, designated by the county prosecutor for ALPR-related responsibilities. A county prosecutor's office utilizing a sheriff's office or public safety agency to maintain ALPR data will have county ALPR Co-coordinators. In this circumstance, a county prosecutor's office is encouraged to allow the sheriff's office or public safety agency the ability to maintain certain ALPR-related responsibilities if the prosecutor's office maintains audit authority.

14. Crime scene query – refers to the process of accessing and reviewing stored non-alert 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.

15. Crime trend analysis – refers to the analytical process by which 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. The 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; or (b) disclosure of personal identifying information concerning any vehicle plate scanned by the ALPR is authorized by a grand jury subpoena. Any crime trend analysis shall document the nature and purpose of the crime trend analysis; the authorized users who accessed stored non-alert data; the designated supervisor who approved access; and 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.

16. 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, regardless of whether 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.

17. Designated supervisor – means an ALPR authorized user, assigned by the Chief of Police who can approve access to crime trend analysis and the disclosure of personal identifying information. The Chief of Police can appoint multiple designated supervisors.

18. Digital License Plate (DLP) – refers to a permanent, vehicle-mounted electronic vehicle license plate updated via cellular phone that emits a radio signal for tracking and digital monitoring purposes. Note: Eight states currently allow residents to opt in to using DLPs. Recently, legislation to allow use in NJ has been introduced.

19. Handheld ALPR – refers to a handheld device with loaded ALPR-based software.

20. Immediate alert – refers to an alert that occurs when a scanned license plate matches the license plate on an initial 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.

21. Law Enforcement ALPR Data – refers to data collected by ALPRs deployed by law enforcement.

22. Mobile ALPR – refers to an ALPR camera(s), contained within this agency's MVR system.

23. Non-encounter alert – refers to an immediate alert when 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.

24. NJ's ALPR Data Sharing Agreement – refers to *New Jersey Attorney General Directive 2022-12*, which is a data sharing agreement between any state, county, and local law enforcement agency and/or authority operating in NJ, which allows unfettered access into ALPR captured read data and amongst law enforcement agencies.

25. NJ CAP5 – (The New Jersey Crime Analysis, Precision Policing and Precision Prosecution Program) - refers to a web application system, powered by *Backtrace* and on which NJ SNAP is found, that provides the ability to search for offenders and suspects within the numerous interconnected law enforcement information streams.

26. NJ SNAP (New Jersey's Statewide Networked ALPR Program) – refers to the interconnected, state ALPR technological framework to establish access to all NJ LE ALPR data and the interface which allows authorized users to query all current and historical connected ALPR data.

27. Permanent fixed ALPR – refers to ALPR camera(s), traditionally referred to simply as fixed, that is deployed in a way that it is not easily moved.

28. Personal identifying information (PII) – is defined as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. PII refers to 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. This includes data comprising a BOLO list and information gained by comparison to the Motor Vehicle Commission (MVC) database or any other data system. This includes data comprising a BOLO list and information gained by comparison to the Motor Vehicle Commission database or any other data system.

29. Point of Interest (POI) – refers to a person and/or vehicle designated on a POI BOLO list entered by an authorized user. When the POI is created, NJ SNAP pushes the POI to all NJ SNAP certified vendors and immediately returns known locate notifications. After the POI is created, NJ SNAP sends out future notification(s) to the investigator via text or email with near real-time information obtained about any POI. An authorized user must designate a supervisor to create a POI and a copy of the POI information is sent to their designated supervisor. A stolen motor vehicle-related POI expires after 48 hours. All other POIs expire within 30 days unless the authorized user designates an alternate expiration date. POIs can be removed before the expiration date by the authorized user who created the POI, their designated supervisor, or an administrator. POIs can be extended in NJ SNAP by the authorized user who created the POI, their designated supervisor, or an administrator. If not extended, the POI will automatically expire.

30. Portable Fixed ALPR Camera(s) – refers to ALPR camera(s) that are fixed to a moveable object or are easily attached and removed from an immovable object. Examples include ALPR cameras that are attached to a trailer or a quick connect ALPR camera that is easily removed from a fixed object, like a telephone pole.

31. Public-Private Partnership ALPR Data – refers to ALPR data collected by a private entity that has entered a public-private partnership with law enforcement.

32. Scan – refers to the process by which an ALPR automatically focuses on, photographs, utilizes optical character recognition (OCR), or converts to digital text the license plate of a vehicle that comes within the range of the ALPR device "reading" the plate characters.

33. Statewide ALPR Program Coordinator – refers to the coordinator, assigned by the Attorney General, in consultation with the NJSP ROIC Commander, tasked with overseeing the Statewide ALPR Program.

34. State ALPR Repository – refers to the repository of NJSP ALPR data. This repository is owned and maintained by the New Jersey State Police (NJSP) Regional Operations & Intelligence Center (ROIC).

35. Statewide API – refers to NJ SNAP's series of developed APIs (application program interface) that allows real-time access to an agency's stored ALPR data wherever it resides.

36. 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.

II. GENERAL ADMINISTRATION

A. The Chief of Police shall designate an agency ALPR Coordinator who will:

1. Be the external point of contact for agency ALPR-related items such as information sharing and audits,

2. Internally oversee the agency's ALPR program, including training and approving access requests (may delegate approval authority to other supervisors), and

3. Designate authorized users within the agency who can use ALPRs and access stored data (such users must complete the trainings mandated by this general order).

4. Collect the *Information Technology Security Awareness Training Acknowledgment Form* (NJSP S.P. 057 Form) biannually, collect *the Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum Certification* (Form H8) annually, and ensure a national fingerprinting based-record query was completed for all vendor personnel.

5. As needed, complete an *Application for the License Plate Reader (LPR) Program* for access to NCIC and MVC Hotlist when requested by NJ SNAP.

B. As per the Attorney General the State ALPR Coordinator shall design and disseminate training on ALPR technology including the application of the *New Jersey Attorney General Law Enforcement Directive 2022-12* and privacy and security considerations generally that shall be a prerequisite for an individual being designated an authorized user under *New Jersey Attorney General Law Enforcement Directive 2022-12*. Authorized users must complete refresher training every two years, as determined by the State ALPR Coordinator.

C. 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’s use manual, and this general order. ALPRs and ALPR-generated data shall only be used for bona fide public safety purposes.

D. NJ SNAP has been authorized to provide the Hotlists (NCIC and MVC) and NJ SNAP POI directly to ALPR vendors. All vendor personnel who have unescorted access to criminal justice information must:

1. Complete CJIS Security Awareness Training and sign the *Information Technology Security Awareness Training Acknowledgment* (NJSP S.P. 057 Form, *Annex A*) biannually and provide the form to this agency.

2. 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 this agency.

3. Conduct a national fingerprinting-based record query.

4. Any vendor personnel, meeting the criminal justice information requirements listed above, can conduct any authorized administrative or operational ALPR function by request of this agency. Vendor personnel access is subject to audit.

5. Additionally, vendors must provide NJ SNAP with a list of all LE agencies they intend to provide the Hotlists. NJ SNAP will contact the LE agency provided by the vendor 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 agency 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.

E. These procedures apply 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.

F. An ALPR and data generated by an ALPR shall only be used for official and legitimate law enforcement business and should be interpreted and applied to achieve the following objectives:

1. To ensure that data that is captured by an ALPR can only be accessed by appropriate law enforcement personnel and can only be used for legitimate, specified, and documented law enforcement purposes.

2. To ensure that BOLO lists that are programmed into the internal memory of an ALPR or that are compared against stored ALPR data are comprised only of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle’s past location(s) through the analysis of stored ALPR data.

3. To permit a thorough analysis of stored ALPR data to detect crime and protect the homeland from terrorist attack while safeguarding the personal privacy rights of motorists by ensuring that the analysis of stored ALPR data is not used to disclose personal identifying information about an individual unless there is a legitimate and documented law enforcement reason for disclosing such personal information to a law enforcement officer or civilian crime analyst.

4. To ensure that stored ALPR data is purged after a reasonable time to minimize the potential for misuse or accidental disclosure.

G. ALPR shall be used in a consistent manner to assist agency personnel in accomplishing its mission in homeland security, suspect interdiction, stolen property recovery, detection of crime, enforcement of State law and local ordinances, identification of stolen vehicles, stolen license plates, wanted and missing persons, AMBER, SILVER, and MVP Alert assistance, crime prevention and other traffic related matters.

H. Information obtained through ALPR use shall only be released or disseminated in accordance with *NJCJIS User Agreement* protocols, applicable State Statutes, and applicable Court Rules. Unauthorized release of any information obtained through an ALPR is subject to criminal, civil, and administrative sanctions. Vigilant detection reports shall not be shared with anyone outside this agency, except other law enforcement agencies.

I. ALPR is more than an enforcement tool. ALPR should be deployed to capture the license plates of vehicles around a major crime or an area of repeated minor offenses. Captured data can be analyzed and utilized in criminal investigations or in the assignment of staffing based on empirical data.

J. Designated supervisors shall:

1. Provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data,

2. Review and approve requests to access and use stored ALPR data to conduct crime trend analyses and/or to access personal identifying information based upon crime trend analyses, and

3. Ensure compliance with this general order and *New Jersey Attorney General Directive 2022-12*.

K. The Chief of Police shall designate all authorized users. No officer or civilian employee will be authorized to operate an ALPR, or access or use ALPR stored data, unless the officer or civilian employee has received training by the agency on the proper operation of these devices, and on the provisions of this general order and *New Jersey Attorney General Directive 2022-12*. Upon an employee's separation from this agency, the employee's account shall be immediately deactivated

III. DEPLOYMENT OF ALPR

A. An ALPR, and the data it generates, shall only be used for official and legitimate law enforcement purposes. The Chief of Police or their designee must authorize deployment of each ALPR.

B. An ALPR shall only be used to scan license plates of vehicles that are exposed to public view (e.g., vehicles on a public road, street, or that are on private property but whose 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 and related properties.

C. The following data must be shared with the County ALPR Coordinator, who will share the information with the State ALPR Coordinator, prior to installing or relocating a permanent fixed ALPR unit:

1. Camera name (pursuant to convention specified by State ALPR Coordinator)

2. Location (latitude and longitude),

3. Survey provided by ALPR vendor, including projected size of ALPR data, and

4. When deploying or relocating a portable fixed ALPR unit, agencies must provide updated latitude and longitude data to the State ALPR Coordinator.

D. The agency ALPR coordinator shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.

E. An ALPR shall not be deployed unless the deployment has been authorized by the Chief of Police, or designated supervisor, or by the New Jersey Attorney General or designee, or a county prosecutor or designee. Such authorization may be given for repeated or continuous deployment of an ALPR (e.g., mounting the device on a particular agency vehicle, or positioning the ALPR at a specific stationary location), in which event the deployment authorization shall remain in force and effect unless and until rescinded or modified by the Chief of Police or designated supervisor, or the Attorney General or County Prosecutor or designee(s).

F. Sworn officers and civilian employees of this agency may operate an ALPR or access or use ALPR stored data only if the person has been designated as an authorized user by the Chief of Police, or by the New Jersey Attorney General or designee, or a County Prosecutor or designee, and has received training from the agency on the proper use and operation of ALPRs, the requirements of *New Jersey Attorney General Directive 2022-12*, and this general order.

G. Any damage to the ALPR systems or any problems with the operation of an ALPR system should be immediately reported to a supervisor verbally and then documented and forwarded to the Chief of Police and the agency ALPR coordinator.

H. Personnel authorized to use ALPR shall ensure that the system is operating properly every time the vehicle is used for patrol. Officers shall log-in to the system.

I. At the end of the shift, the officer shall log out of the ALPR system until the next time the system is deployed.

IV. MAINTENANCE OF RECORDS

A. The agency ALPR coordinator or their designee shall maintain a written or electronic record that documents the following information. Such information can be automated through the ALPR system.

1. Date and time when the ALPR had been deployed.

2. Whether the ALPR was mobile or was stationed at a fixed specified location.

3. The identity of the operator(s) of the vehicle, as applicable.

4. Whether ALPR data was transferred to any other database or data storage device or system.

5. Vigilant and or Rekor shall maintain the ALPR data storage, the data server, and related storage equipment. Any ALPR device or related equipment related to the devices shall be maintained by the agency coordinator or coordinator's designee.

B. The agency ALPR coordinator or their designee shall maintain a record of all access to stored ALPR data. The agency's ALPR data recordkeeping system, which may be automated, shall document the following information:

1. The date and time of access, and in the case of access to stored non-alert data, the type of access authorized (e.g., BOLO query, crime scene query, or crime trend analysis).

2. A list of authorized users.

3. The authorized user who accessed the stored data.

4. Whether an automated software program was used to analyze stored data.

5. The designated operator who reviewed and approved any disclosure of personal identifying information based upon crime trend analysis when such approval is required.

6. The designated operator who approved any use of an automated crime trend analysis computer program that would automatically alert and disclose personal identifying information; and

7. Any other information required to be documented.

C. By January 31st each year, the agency ALPR coordinator shall perform an audit of this agency's ALPR program and provide it to the Essex County and State ALPR coordinators. Such audit shall certify the following:

1. Agency has an ALPR policy in place consistent with *New Jersey Attorney General's Directive 2022-12.*

2. Only authorized users have accessed ALPR data.

3. Record and date of each authorized user's last ALPR training.

4. That a random survey of ALPR accesses revealed no misuse.

5. That all ALPR vendor personnel accessing criminal justice information have been fingerprinted, provided this agency a signed Information *Technology Security Awareness Training Acknowledgment* (NJSP S.P. 057 Form) biannually and provided a signed Federal Bureau of Investigation, *Criminal Justice Information Services, Security Addendum Certification* (Form H8) annually.

6. That this agency is in CJIS compliance and allowed to receive Hotlists.

7. A description of any known significant violations and citizen complaints and whether they have been forwarded to the Essex County Prosecutor or Director of the New Jersey Division of Criminal Justice.

D. The annual ALPR audit date range is January 1 through December 31 of the same year. The agency ALPR coordinator will conduct an audit of ALPR access for ALPR searches, BOLO entries, and NJ SNAP Point of Interest (POI) entries for every ALPR vendor utilized by this agency. The random sampling of ALPR access for ALPR searches and separately, BOLO entries and POI entries, will be conducted in the following manner:

1. The agency ALPR coordinator or their designee(s) will export a list of all users' ALPR searches, BOLO entries and POI entries.

2. Once exported, the list's data rows will be randomized before review.

3. At a minimum, the agency ALPR coordinator will review 1% of this agency's ALPR searches, BOLO entries, and POI entries to ensure that Username/ID, date and time, purpose, justification, and legitimate law enforcement report number are captured and valid.

   a. For a POI entry, the identified supervisor must also be reviewed for validity.

   b. The agency ALPR coordinator is encouraged to review additional ALPR searches, BOLO entries, and POI entries beyond the 1% threshold.

4. If this agency conducted less than 100 ALPR searches, BOLO entries, and/or POI entries during the audit period, the agency ALPR coordinator must review no less than 5 of each.

5. To ensure public trust, protect civil liberties and prevent misuse, the agency ALPR coordinator is encouraged to conduct periodic and random samplings of ALPR use outside this annual audit.

6. By midnight on January 31 of the following year, the agency ALPR coordinator must certify the audit through the Office of Public Integrity & Accountability law enforcement web portal.

7. To ensure public trust, protect civil liberties and prevent misuse, the Chief of Police may cause periodic and random samplings of ALPR use outside the annual audit.

8. If a minor violation of the audit parameters is discovered during the audit, the agency ALPR coordinator shall follow this agency's policies and procedures on remedial training to remediate the violation. Minor violation examples include a user:

   a. Unintentionally selecting the wrong purpose or justification.

   b. Placing valid information in the wrong required field.

   c. Not providing the full law enforcement report number.

9. If a significant violation is discovered during the audit, see XIII of this policy Significant violation examples include a user:

   a. Who does not have authorized access to ALPR data utilizing it.

   b. Sharing or allowing other individuals to use a username/ID other than the one assigned.

   c. Utilizing ALPR data or a BOLO for an unauthorized purpose

10. The agency ALPR coordinator will keep a copy of the audit and all random sampling data for 3 years from the first day of the audit certification period (e.g., since the certification period for 2023 data is from January 1-31, 2024, the audit copy and data must be retained from January 1, 2024, until January 1, 2027).

E. All written or electronic records of ALPR activity and access to ALPR data shall be maintained for a period of three years and shall be kept in a manner that makes such records readily accessible to any person authorized by this general order to audit the agency's use of ALPRs and ALPR generated data. If an automated system is used to record any information that is required to be documented pursuant to this general order, it shall not be necessary to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.

F. All stored data and required documentation and decisions shall be kept in a place and in a manner as to facilitate a review and audit of the agency's ALPR program by the Essex County Prosecutor’s Office or by the New Jersey Attorney General or designee(s).

IV. CONTENT AND APPROVAL OF BOLO LISTS

A. 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 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:

1. Persons who are subject to an outstanding arrest warrant.

2. Missing persons.

3. AMBER/SILVER/MVP alerts.

4. 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.

5. Stolen vehicles

6. Vehicles reasonably believed to be involved in the commission of a crime or disorderly persons offense.

7. 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.

8. Vehicles with expired registrations or other N.J.S.A. 39:1-1 et seq. violations.

9. 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.

10. Persons wanted by a law enforcement agency who are of interest in a specific investigation, regardless of whether such persons are themselves suspected of criminal activity.

11. Persons who are on any watch list issued by a state or federal agency responsible for homeland security.

B. 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, United States Department of Homeland Security, and Motor Vehicle Commission database.

C. 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 agency vehicles, and as frequently as possible, but at least daily, for ALPRs at stationary locations.

D. All ALPR systems must provide an Application Program Interface (API) or web service to update in real-time a BOLO list(s) through methods approved by the State ALPR Coordinator, including AMBER/SILVER/MVP alerts that remain on the list until expired or withdrawn.

V. ACTIONS IN RESPONSE TO AN IMMEDIATE ALERT

A. 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 officers should not encounter the vehicle) and, if so, follow any instructions included in the alert for notifying the originating agency.

B. When officers receive an immediate alert, the officer shall take such action in response to the alert as is appropriate in the circumstances. Officer(s) alerted to the fact 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 in the vehicle before the officer would have a lawful basis to stop the vehicle. (*State v. Parks*, 288 N.J. Super. 407 App. Div. 1996). Officers do not have reasonable suspicion to justify a stop based on a computer check that shows that the operator's license of the registered owner of the vehicle is suspended unless the driver generally matches the owner's physical description (e.g., age and gender).

C. An officer reacting to an immediate alert shall consult the database to determine the reason why the vehicle had been placed on the BOLO list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO.

VI. STORAGE AND SECURITY OF ALPR DATA

A. 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. 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.

1. The agency ALPR coordinator or his/her designee shall maintain an automated record-keeping of all access to stored ALPR data, including the following information, unless specified differently below.

2. The date and time of access, and in the case of access to stored non-alert data, the type of access authorized (e.g., BOLO query, crime scene query, or crime trend analysis).

3. The authorized user who accessed the stored data.

4. Whether an automated software program was used to analyze the data.

5. Designated supervisor who approved disclosure of personal identifying information based upon crime trend analysis.

6. Instances of testing or troubleshooting an ALPR system.

7. Any other information required to be documented under this general order.

B. All ALPR stored data shall be kept in a secure data storage system with access restricted to authorized persons. Access to this stored data shall be limited to the purposes described in Section IX of this general order.

C. Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data to ensure that access to and use of non-alert data and any disclosure of personal identifying information resulting from the analysis of non-alert data occurs only as authorized pursuant to Section IX of this general order. Positive alert data may, as appropriate, be transferred to the appropriate active investigation file and if appropriate be placed into evidence in accordance with the agency's evidence or records management procedures.

VII. RETENTION PERIOD AND PURGING OF STORED DATA

A. ALPR stored data shall be retained for a period of three (3) years, after which, the data shall be purged from the agency's data storage device or system.

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 the three-year retention and purging schedule established in *New Jersey Attorney General Directive 2022-12.*

VIII. LIMITATIONS ON ACCESS TO AND USE OF STORED ALPR DATA

A. Authorized users may access and use stored ALPR Alert Data 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.

1. A record shall be made of all access to ALPR data, which may be an automated record that documents the date of access and the identity of the authorized user and for non-alert data the record should include the justification for access. Once stored data has been accessed and transferred to an investigation file by an authorized user, it shall not be necessary after that to document further access or use of that data pursuant to *New Jersey Attorney General Law Enforcement Directive 2022-12*.

2. An authorized user does not need to obtain approval from the Chief of Police or designated supervisor for each occasion on which he or she accesses and uses stored ALPR data. Once positive alert data has been accessed and transferred to an investigation file, it shall not be necessary thereafter to document further access or use of that data pursuant to this general order.

B. Access to and use of stored Non-Alert ALPR Data is limited to the following three purposes:

1. A BOLO query.

2. A crime-scene query.

3. Crime trend analysis (system test and troubleshooting are also acceptable purposes).

C. An authorized user does not need to obtain approval from the Chief of Police or a designated supervisor for each occasion on which he or she accesses and uses stored non-alert data pursuant to this general order.

D. BOLO Query – Authorized users 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).

E. Crime Scene Query – Authorized users 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.

F. Crime Trend Analysis – Authorized users 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; or (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

b. The authorized users who accessed stored non-alert data

c. The designated supervisor who approved access

d. When 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.

G. For the purposes of this section, the specific and articulable facts that warrant further investigation standard required for the disclosure of personal identifying based upon crime trend analysis of stored non-alert data is intended to be comparable to the specific and articulable facts that warrant heightened caution standard developed by the New Jersey Supreme Court in *State v. Smith*, 134 N.J. 599, 616-19 (1994) (establishing the level of individualized suspicion required before an officer may order a passenger to exit a motor vehicle stopped for a traffic violation).

IX. SHARED LAW ENFORCEMENT ACCESS TO STORED ALPR DATA

A. Statewide API – As per the Attorney General 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.

B. Agencies may also share data regionally with other New Jersey agencies pursuant to the mandates of this general order, 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 and newly acquired 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.

C. As per the Attorney General 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 general order 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 to achieve the objectives of this general order. Private entities may provide ALPR data to New Jersey agencies but cannot receive law enforcement-owned ALPR data.

D. Stored ALPR data may be combined with ALPR data collected by two or more law enforcement agencies (e.g., collection of stored data by the State Police Regional Operations Intelligence Center); provided that such aggregated data shall only be retained, accessed, and used in accordance with the provisions of *New Jersey Attorney General Directive 2022-12* and this general order.

E. When ALPR data is made accessible to or otherwise shared with or transferred to another law enforcement agency, the ALPR Coordinator shall document the identity of the other agency and the specific officer(s) or civilian employee(s) of that agency who were provided the information and ensure that the other agency has an approved ALPR policy.

X. DISCOVERY

A. Criminal investigatory records

1. Stored ALPR data shall be treated as criminal investigatory records within the meaning of N.J.S.A. 47:1A- I 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.

2. Upon 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)).

B. Release of ALPR data.

1. 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).

2. If the investigation results in criminal charges, the ALPR records shall be turned over in discovery pursuant to applicable court rules and case law.

XI. COMPLIANCE

A. The Chief of Police shall provide a copy of this general order to the Essex County Prosecutor and County and State ALPR Coordinators at or before the time of promulgation, including any subsequent policy amendments.

B. Violations

1. Any knowing violation of this general order or related agency standing operating procedure, policy, order, or applicable law, shall be subject to discipline.

2. All significant violations of this general order, including but not limited to unauthorized access or use of ALPR stored data, must be reported to the County Prosecutor and County and State ALPR Coordinator upon discovery. Unless the County Prosecutor or Director of the Division of Criminal Justice 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 Chief of Police and with notification to the State ALPR Coordinator, explaining to the County Prosecutor or to the Director of the Division of Criminal Justice, the circumstances of the violation, and the steps that are being taken to prevent future similar violations.

3. Any complaints about an agency’s ALPR program made by any person or entity shall be forwarded to the Essex County Prosecutor for appropriate review and handling, as well as notification to the County and State ALPR Coordinator. The County Prosecutor or Director of the Division of Criminal Justice may investigate or direct the agency that is the subject of the complaint to investigate and report back to the County Prosecutor, with notification to the State ALPR Coordinator.

4. The County ALPR Coordinator shall maintain a record of any reports of significant violations and public complaints to include:

a. Those made directly to the County Prosecutor’s Office,

b. Those made directly to any law enforcement agency in the respective county, and

c. Those made directly to any agency falling under the County ALPR Coordinator’s responsibility.

5. The County ALPR Coordinator or State ALPR Coordinator may conduct an audit of an agency’s ALPR program at any time.

XII. SANCTIONS FOR NON-COMPLIANCE

A. If the Attorney General, County Prosecutor or designee has reason to believe that this agency, officer, or civilian employee is not complying with or adequately enforcing the provisions of New Jersey Attorney General's Directive 2022-12, 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.

B. The Attorney General or designee may initiate disciplinary proceedings and may take such other actions as the Attorney General in his or her sole discretion deems appropriate to ensure compliance with this general order.

XIII. AUTHORITY OF ATTORNEY GENERAL TO GRANT EXEMPTIONS OR SPECIAL USE AUTHORIZATIONS

A. ALPRs, and all ALPR stored data, shall only be used and accessed as authorized by this general order. However, the Attorney General or their designee may authorize the specific use of an ALPR or the data it generates that is not expressly authorized by this general order. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by this general order shall be made to the Attorney General or their designee through the DCJ Director.

B. Such requests shall be made in writing unless the circumstances are exigent, in which case approval or denial may be given orally and memorialized in writing as soon thereafter as is practicable.

XIV. CYBERSECURITY BEST PRACTICES

A. As per the New Jersey Statewide ALPR Coordinator, this agency shall implement cybersecurity best practices and controls that reasonably conform to the most recent version of one or more of the following industry-recognized cybersecurity control families:

1. The New Jersey Statewide Information Security Manual; or

2. The Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

3. The Criminal Justice Information Security Policy

B. ALPR security standards must specifically address supply chain risk management, configuration management, and physical access control.

XV. SUPPLY CHAIN RISK MANGEMENT

A. This agency shall implement supply chain risk management (SCRM) processes to help protect system components, products, and services that are part of ALPR systems and infrastructures. SCRM controls help ensure that security and privacy requirements, threats, and other concerns are addressed throughout the ALPR system's life cycle and the national and international supply chains.

B. To mitigate supply chain risks, this agency shall comply with Section 889 of Public Law 115-232, the John S. McCain National Defense Authorization Act, and 2 CFR 200.216, which prohibits agencies from obligating or expending federal grant funds to:

1. Procure or obtain; or

2. Extend or renew a contract to procure or obtain; or

3. Enter a contract (or extend or renew a contract) to procure or obtain systems, equipment or services that include components from the following companies:

   a. Huawei Technologies Company.

   b. ZTE Corporation.

   c. Hytera Communications Corporation.

   d. Hangzhou Hikvision Digital Technology Company.

   e. Dahua Technology Company.

   f. Any of subsidiaries or affiliates of these companies.

B. Supplemental Guidance: An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. This agency can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. This agency should review the US Department of Commerce Bureau of Industry and Security Lists of Parties of Concern, the International Trade Association Consolidated Screening List, and the National Defense Authorization Act (NDAA) Section 889 prior to contracting with a supplier. In general, the NJ Office of Homeland Security and Preparedness prohibits agencies from purchasing systems, system components, and services from companies on these lists due to threats they pose to the State and/or Nation. This agency should contact the NJCCIC for further guidance.

XVI. ALPR CONFIGURATION MANAGEMENT

A. This agency shall establish, document, and implement security configuration settings of ALPR systems that reflect the most restrictive mode consistent with their operational requirement. Each ALPR system and component shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: Endpoint Detection and Response (EDR) software and security event logging, as feasible.

1. **Supplemental Guidance:** Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (1) registry settings; (2) account, file, directory permission settings; and (3) settings for functions, ports, protocols, services, and remote connections. Common secure configurations

can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors. Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. This agency may refer to the following resources for common security configuration settings.

Center for Internet Security (CIS) benchmarks:
https://benchmarks.cisecurity.org/downloads/benchmarks/

United States government configuration baselines:
https://csrc.nist.gov/projects/united-states-government-configuration-baseline

NIST recommended configurations and checklists:
http://checklists.nist.gov/

National Security Agency (NSA) configuration guides:
https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm

XVII. PHYSICAL SECURITY

A. This General Order establishes physical controls and procedures that limit access to ALPR systems, equipment, and the respective operating environments to only authorized individuals.

XVIII. OTHER SECURITY BEST PRACTICES

A. To ensure ALPR-related devices are secure, the following best practices should be adhered to:

1. Always operate services exposed on internet-accessible hosts with secure configurations.

2. Never enable external access without compensating controls such as boundary firewalls and segmentation from other more secure and internal hosts like domain controllers.

3. Continuously assess the business and mission need of internet-facing services.

4. Follow best practices for security configurations, especially blocking macros in documents from the internet.

5. It is imperative that Internet of Things (IoT) devices are logically or physically segmented from the organization's other networks. Doing so will reduce the risk of a successful attack against an IoT device of causing cascading impacts across the organization.