SUSSEX COUNTY PROSECUTOR'S OFFICE Standard Operating Procedure			
VOLUME: 1	**CHAPTER:**	**# OF PAGES: 18**	
SUBJECT: AUTOMATED LICENSE PLATE RECOGNITION (ALPR)			
EFFECTIVE DATE: **1/23/2023**	**ACCREDITATION STANDARDS:**	**REVISION DATE**	**PAGE #**
BY THE ORDER OF: **Acting Prosecutor Annmarie Taggart**			
SUPERSEDES ORDER #:			

PURPOSE The purpose of this directive is to establish a uniform policy and procedure for the use of automated license plate recognition (ALPR).

POLICY It is the policy of the Sussex County Prosecutor's Office to utilize ALPR technology to the extent possible in accordance with New Jersey Attorney General's Directive 2022-12.

PROCEDURES

I. Definitions

Agency ALPR Coordinator - is the main point of contact within a law enforcement or public safety agency or authority, designated by the law enforcement executive 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 (such users must complete the trainings mandated by this Directive). An agency may also have a co-coordinator(s).

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

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 police squad cars.

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

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.

Attorney General Law Enforcement Directive No. 2022-12 - Updated Directive Regulating Use of Automated License Plate Recognition (ALPR) Technology) – also known as "the Directive."

Authorized User – means 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 Offices can be authorized users. Authorization shall be given by the Agency ALPR Coordinator for each respective agency.

Automated License Plate Recognition (ALPRs) – 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 police vehicle and capable of operating while the vehicle is in motion.

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.

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. The list is typically provided in a comma-separated value (CSV) format or other delimited file that 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.

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

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

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

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 Department 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 Department or Public Safety Agency the ability to maintain certain ALPR-related responsibilities as long as the Prosecutor's Office maintains audit authority.

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.

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.

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.

Designated Supervisor – means a superior officer, who is an ALPR "authorized user", assigned by the Agency ALPR Coordinator who can approve access to crime trend analysis and the disclosure of PII. A law enforcement agency may have more than one designated supervisor.

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.

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

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.

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

Mobile ALPR – refers to an ALPR camera(s), mounted on a motor vehicle.

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.

NJ's ALPR Data Sharing Agreement – refers to 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.

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.

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.

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. For example, an ALPR camera that is permanently affixed to an overhead sign structure over a roadway.

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.

Point of Interest (POI) – refers to a person or vehicle designated 1) to be searched for in stored ALPR data in NJ SNAP, and; 2) to trigger a notification in the event of a future ALPR scan. Notification of ALPR scan(s) are sent to the investigator via text or email. A POI can be created in NJ SNAP by an authorized user with the approval of a designated supervisor. A POI pertaining to a stolen motor vehicle expires in 48 hours. All other POIs expire in 30 days. POIs can either be removed before the expiration date, or extended, by the authorized user who created the POI (with approval of a designated supervisor), a designated supervisor or an administrator.

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.

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.

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.

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).

Statewide API (Application Program Interface) - 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.

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. Oversight

A. **Agency.** The law enforcement executive of each agency using an ALPR or its data 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 ALPR program, including training and approving access requests (may delegate approval authority to other supervisors);

3. Designate authorized users within the agency who can use ALPRs and access stored data (such users must complete the trainings mandated by New Jersey's Attorney General Directive 2022-12).

B. **County.** Each County Prosecutor's Office will designate a County ALPR Coordinator who will maintain contact information for Agency ALPR Coordinators in the county and provide it to the State ALPR Coordinator. Where county ALPR data is maintained by a sheriff's department or public safety agency, a representative from that agency may be designated as a County ALPR Co-Coordinator. State agencies should report their Agency ALPR Coordinator directly to the State ALPR Coordinator.

C. **State.** The Attorney General, in consultation with the New Jersey State Police ROIC Commander, will designate a State ALPR Coordinator to oversee the "Statewide API" that connects stored ALPR data and the state's ALPR program.

III. General

A. 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.

1. ALPRs and ALPR-generated data shall only be used for bona fide public safety purposes to include use 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.

B. These procedures apply to any ALPR data that is collected by another law enforcement agency and provided to this Office or collected by this Office and provided to another law enforcement agency. For additional procedures on shared law enforcement data see Section XI.

C. 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 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;

2. 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;

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 as a means 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; and

4. To ensure that stored ALPR data are purged after the mandatory retention length of three years, unless it is associated with an active investigation or pending judicial process as to minimize the potential for misuse or accidental disclosure.

D. ALPR shall be used in a consistent manner to assist department 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 Alert assistance, crime prevention and other traffic related matters.

E. 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.

F. ALPR is more than an enforcement tool. ALPR should be deployed to capture the license plates of vehicles in the area of 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.

G. County ALPR Coordinator shall:

1. Maintain contact information of Agency Coordinators and provides to State Coordinator by January 15 each year;

2. Aid Agency Coordinators with deconflicting ALPR deployment locations;

3. Collect Agency ALPR policies and forward the to State Coordinator;

4. Collect significant violation reports and citizen complaints, then forward to County Prosecutor and State Coordinator within 7 days;

5. Assist in external sharing with LE agencies outside NJ or otherwise not covered by Directive Agency audits received by Jan. 31 annually, then forward to State Coordinator may audit an agency's ALPR program at any time; and

6. Starting in 2024, for calendar year 2023, report via OAG LE Reporting Portal all alleged and sustained violations, alleged and sustained citizen complaints, and a list of agencies who completed audits.

H. The Agency ALPR Coordinator 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 New Jersey's Attorney General's Directive 2022-12.

IV. Deployment of ALPR

A. **Official use only.** An ALPR and the data it generates shall only be used for official and legitimate law enforcement purposes. The agency's law enforcement executive or designee must authorize deployment of each ALPR.

B. **Scanning limited to vehicles exposed to public view.** 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 parking lot of a shopping mall or other business establishment).

C. **Sharing deployment information.** The following data must be shared with the State ALPR Coordinator prior to installing or relocating a permanent fixed ALPR unit:

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

2. Location (latitude and longitude); and the

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

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

D. **Deconfliction**. Agency ALPR Coordinators shall deconflict with the County and State ALPR Coordinator about deployment locations to avoid duplication of efforts.

E. An ALPR shall not be deployed in the field unless the deployment has been authorized by the Chief or a designated supervisor, or by the 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 police 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 or designated supervisor, or the Attorney General or County Prosecutor or designee(s).

F. Authorized users of the agency may operate an ALPR or access or use ALPR stored data only if the person has been designated as such by the law enforcement executive of the agency, by the County Prosecutor or his/her designee, or by the Attorney General or his/her designee and has received training from the agency on the proper use and operation of ALPRs, the requirements of Attorney General Law Enforcement Directive 2022-12, and this policy.

G. Personnel must ensure that the lenses are free from obstructions before operations. If safe to do so, personnel may remove obstructions such as snow, mud, paper, etc. Under no circumstances are the camera lenses to be wiped with anything other than a clean, soft cloth.

H. 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 on an Inter-Office Memorandum and forwarded to the Chief.

I. Personnel authorized to use the ALPR shall ensure that the system is operating properly every time the system is used. Officers shall sign on to the system in the following manner:

1. All officers shall log on using his/her individually assigned, unique login name.

2. All officers shall log on using his/her assigned password.

3. Generic or shared login information is not permitted.

V. Maintenance of Records

A. The Agency ALPR Coordinator shall maintain a written or electronic record that documents the following information for each agency-owned ALPR unit:

1. Date and time when the ALPR was deployed;

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

3. The identity of the operator(s); and

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

B. All written or electronic records of ALPR activity and access to ALPR data shall be maintained by the agency 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 directive 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 directive, it shall not be necessary to maintain duplicate records of any events or transactions that are documented by the automated record-keeping system.

C. 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 County or State ALPR Coordinators, by the County Prosecutor or designee(s), or the Attorney General or designee(s).

VI. Content and Approval of BOLO Lists

A. **Standard for including license plate in a BOLO List.** A license plate 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 exist) 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.

B. 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 or Silver 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 that are reasonably believed to be involved in the commission of a crime or disorderly persons offense;

7. Vehicles that are registered to or are 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 Title 39 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, whether or not such persons are themselves suspected of criminal activity; and

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

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

D. **Updating BOLO list**. 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.

1. 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 alerts that remain on the list until expired or withdrawn.

VII. 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 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 NJ. Super (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) 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.

VIII. Security of Stored ALPR Data

A. 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.

B. Stored ALPR data shall be maintained electronically in such a manner as to distinguish alert data from non-alert data so as 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. 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.

IX. Storage, Records, and Retention

A. ***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.

B. ***Deployment records***. Agencies shall maintain the following information regarding each ALPR owned or operated:

1. Date and time deployed;

2. Portable or fixed;

3. Identity of operator;

4. Vendor name; and

5. Date ALPR data connected to Statewide API (for agencies that house ALPR data).

C. ***Stored ALPR data access records***. Agencies that store ALPR data shall maintain an automated record-keeping of all access to stored ALPR data (in the case of county storage, the county may keep access records instead), including the following:

1. Date and time of access, and for non-alert data, the justification for access;

2. Authorized accessor name;

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

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

5. Instances of testing or troubleshooting an ALPR system; and

6. Any other information required to be documented under this Directive.

D. ***Retention***. Records and ALPR data covered by this Section shall be retained for three years.

1. 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.

2. 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.

3. Records shall be kept in a manner that makes them readily accessible for audit.

X. 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.

2. An authorized user does not need to obtain approval from the Chief or designated supervisor for each occasion on which he or she accesses and uses stored ALPR alert 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 directive.

B. 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 a crime trend analysis (system test and troubleshooting are also acceptable purposes).

C. **BOLO Query**

1. 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).

D. **Crime Scene Query**

1. 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.

2. A crime scene query shall be limited in scope to data that is reasonably related to the specified criminal event, considering the date, time, location, and nature of the specified criminal event. For example, a crime that reasonably involves extensive planning and possible “rehearsals,” such as a terrorist attack, would justify examining data that had been scanned and collected days or even weeks or months before the criminal event and that may have been scanned at a substantial distance from the site of the crime or intended crime (e.g., at any point along a highway leading to the intended crime site). In contrast, a spontaneous crime might reasonably justify examining data that was scanned and collected on or about the time of and in closer physical proximity to the criminal event.

E. **Crime Trend Analysis**

1. 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.

2. 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.

3. 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).

4. Any crime trend analysis shall document:

   a. The nature and purpose of the crime trend analysis;

   b. The persons who accessed stored non-alert ALPR data for use in conducting that analysis; and

   c. The designated supervisor who approved access to ALPR non-alert data;

   d. 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.

F. ***Documenting access for any stored data search***. A record shall be made of the authorized user accessing stored ALPR data and the date, 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.

XI. Shared Law Enforcement Access to Stored ALPR Data

A. **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 2022-12, which is January 23, 2023, 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.

B. **Sharing with agencies not covered by Attorney General Law Enforcement 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.

C. 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 AG Directive 2022-12 and this directive.

D. 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.

XII. Discovery

A. 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.

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. Any County Prosecutor's Office 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 Director of the Division of Criminal Justice (DCJ).

B. **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.

XIII. Compliance

A. **Establishing a policy**. Agencies that possess or use an ALPR or its data shall establish—or conform existing—standing operating procedures, directives, or orders that govern ALPRs and stored ALPR data consistent with this Directive before the Directive takes effect (ninety days after issuance). The law enforcement executive shall provide a copy of the agency's ALPR policy to the County Prosecutor (County Prosecutor's Office shall report to the DCJ Director) and County and State ALPR Coordinator at or before the time of promulgation, including any subsequent policy amendments.

B. The County ALPR Coordinator shall provide a copy of this policy and/or New Jersey's Attorney General Directive 2022-12 to the County Prosecutor and State ALPR Coordinator at or before the time of promulgation and shall provide to the County Prosecutor and State ALPR Coordinator copies of any amendments or revisions to this policy at or before the time that such amendments take effect.

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

1. All significant violations of this 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.

2. 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. **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. That audit shall certify the following:

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

1. Once the Agency ALPR Coordinator submits their audit to their County ALPR Coordinator by January 31 each year, the County Coordinator must forward it to the State ALPR Coordinator.

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

D. **Training**. 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 Directive 2022-12. Authorized users must complete refresher training every two years, as determined by the State ALPR Coordinator.

XIV. Sanctions for Non-Compliance

A. If the Attorney General, County Prosecutor or designee has reason to believe that a law enforcement agency or 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. 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 Directive.

XV. Authority of Attorney General to Grant Exemptions or Special Use Authorizations

A. **Attorney General exemptions**. ALPRs, and all ALPR stored data, shall only be used and accessed as authorized by this Directive. 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 Directive. Any request by a department to use an ALPR or ALPR-generated data for a purpose or in a manner not authorized by this Directive shall be made to the Attorney General or their designee through the DCJ Director. 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.

XVI. Statewide Information Security Manual (SISM) Supply Chain, Configuration Management, and Cybersecurity Best Practices

As per the New Jersey Statewide ALPR Coordinator, agencies 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;
(2) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or
(3) the Criminal Justice Information Security Policy

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

XVII. Supply Chain Risk Management

Agencies 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.

To mitigate supply chain risks, agencies 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:

A. Procure or obtain;
B. Extend or renew a contract to procure or obtain; or
C. Enter into a contract (or extend or renew a contract) to procure or obtain systems, equipment or services that include components from the following companies:
    - Huawei Technologies Company,
    - ZTE Corporation,
    - Hytera Communications Corporation,
    - Hangzhou Hikvision Digital Technology Company,
    - Dahua Technology Company, and
    - any of subsidiaries or affiliates of these companies.

.

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.

Agencies can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits.

Agencies 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. Agencies should contact the NJCCIC for further guidance.

XVIII. ALPR Configuration Management

Agencies 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.

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: (i) registry settings; (ii) account, file, directory permission settings; and (iii) 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.

Agencies 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

XIX. Physical Security

Establish physical controls and procedures that limit access to ALPR systems, equipment, and the respective operating environments to only authorized individuals.

XX. Other Security Best Practices

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.