NORTH CAROLINA
STATE BUREAU OF INVESTIGATION

3320 Garner Road
Raleigh, NC 27610
(919) 662-4500
FAX: (919) 662-4523

JOSH STEIN
GOVERNOR

R. E. "CHIP" HAWLEY
DIRECTOR

September 22, 2026

MEMORANDUM

To: Law Enforcement Agency Heads

From: R.E. "Chip" Hawley, Director REH

Subject: Best Practices for Law Enforcement ALPR Programs in North Carolina

The purpose of this memorandum is to provide your agency with the attached Best Practices for Law Enforcement ALPR Programs in North Carolina guidance, which has been developed as a resource to assist law enforcement agencies in establishing, reviewing, and enhancing policies, procedures, and operations practices related to ALPR systems operating in North Carolina.

ALPR technology has been instrumental in assisting law enforcement with protecting the public and solving crimes across our state and nation. It is an investigative tool that requires strong governance controls to ensure that it is being utilized appropriately by those with access. It is critically important that you conduct internal audits of these systems so that any misuse is immediately identified and addressed.

This guidance is intended to provide practical considerations and recommended practices that agencies may use in evaluating current operations and determining whether enhancements or modifications are appropriate. It is not intended to establish mandatory requirements; rather it is designed to serve as a resource that agencies may adapt based on individual missions, operational environments, and community needs. We recognize that law enforcement agencies vary significantly in size, structure and jurisdiction and may utilize various vendors to provide ALPR services. Agency heads are encouraged to review the best practices and determine which recommendations may be appropriate to incorporate into their respective policies, procedures, training, oversight and operational practices.

This guidance was developed in partnership with the NC Sheriffs' Association, NC Association of Chiefs of Police, and the NC Police Executives Association. We appreciate their continued collaboration to ensure best practices in this area across our state.

Thank you for your continued leadership and commitment to promoting professionalism, accountability, and effective law enforcement services. Please let me know if we can answer any questions that you may have and feel free to contact me at any time.

Best Practices for Law Enforcement ALPR Programs in North Carolina

Automatic License Plate Reader (ALPR) technology can be an invaluable investigative and public-safety tool, but it must have strong governance controls. These are recommended best practices for agencies to ensure that the technology is being used for the sole purpose of public safety while recognizing the privacy interests of their citizens. These best practices are intended for agencies that own and operate ALPR cameras and maintain data from ALPR cameras. It is critical that agencies review and follow Article 3D of Chapter 20 of the North Carolina General Statutes as they set up and implement an ALPR program.

In addition to the following best practices, agencies may wish to consider maintaining and periodically aggregating key information regarding ALPR system usage, including general investigative outcomes, the number of system searches conducted, documented instances of misuse, and examples of successful investigative applications. Maintaining this information may assist agencies in responding to inquiries from government officials, community members, or other stakeholders regarding the use, effectiveness, oversight, and accountability of ALPR technology.

1. Establish a clear policy framework

A detailed written ALPR policy is required by G.S. § 20-183.31. This statute includes several topics that the policy should address. The grid below contains the topics required by the statute, as well as additional topics that it would be beneficial for the policy to address.

The policy must be adopted before the system becomes operational and clearly define:

Purpose and authorized uses	Supervisory oversight and review
Prohibited uses	Auditing
Authorized users	Security and access controls
Types of databases/hot lists	Vendor responsibilities
Real-time alerts	Maintenance and calibration
Historical searches	Procedures for inaccurate plate reads
Search justification requirements	Procedures for system alerts
Data retention	Complaints and misuse
Data sharing with law enforcement agencies	Periodic program evaluation
Training	Alert-response protocol

This technology is constantly evolving so policies should be regularly reviewed and revised. Agencies may want to consider developing a separate governing document or Standard Operating Procedure (SOP) that can be updated immediately as changes are made.

2. Clearly distinguish an ALPR "hit" from probable cause or reasonable suspicion

An ALPR alert is an investigative lead only. It, by itself, does not establish probable cause as it is not confirmation that a vehicle or person is involved in criminal activity. Officers must independently verify an ALPR alert before taking enforcement action. This is especially important because of optical character recognition errors, stolen plates, plate changes, database delays, and similar vehicles can generate false positives.

Officers should independently verify:

License plate number	Time/location
State/jurisdiction	Source database
Vehicle description	Whether the plate is still wanted
Plate status	Whether circumstances support the alert

3. Establish strict rules for conducting system searches

Historical ALPR searches are potentially more intrusive than receiving an alert.
A strong policy should require the user to document:

Case/event number	Date/time range
Investigative purpose	Geographic area
Offense or incident	User conducting the search
Specific investigative nexus	Results/action taken
Search parameters	

Agencies may consider requiring one of the following controls:

1. Require the above parameters to be emailed to a detective or supervisor prior to the search for approval.
2. Limit access to ALPR databases to supervisors and/or detectives.
3. Require supervisor approval for broad or sensitive searches, such as large geographic areas, extended time periods, or constitutionally protected activities. E.g., if an ALPR search has the potential to capture information on First Amendment protected activity, such as a protest or assembly.

4. Set data retention limits

Collect and retain only what your agency legitimately needs. Agencies should ensure that they are following all procedures listed in G.S. § 20-183.32, which states that captured plate data shall not be preserved for more than 90 days after the date the data is captured, unless an applicable statutory exception applies, such as a qualifying preservation request or a search warrant. A particularly good agency practice is to make the retention period

shorter than the statutory maximum when operationally feasible. Agencies should discuss data retention with their vendor(s) prior to use of the system. Some vendors have settings that allow an agency to select retention periods less than the 90 days required by NC law. Evidence obtained from databases may be retained in an agency's evidence system if it is part of a criminal investigative case file.

5. Control access using role-based permissions

Not every employee should have unrestricted ALPR access. Consider access permissions based on roles.

ROLE	EXAMPLE ACCESS
Patrol officer	Real-time alerts/limited searches
Investigator	Case related historical searches
Supervisor	Search review/approval
ALPR system administrator	System administration
Analyst	Approved searches for analytical reasons
Auditor	Read only audit access
IT/Security	Technical administration without investigative access

Access should be immediately removed when an employee transfers, retires, resigns, is suspended, changes duties, or no longer has a legitimate need. The policy should designate who within the agency is responsible for completing these actions.

6. Require a reason for every search

G.S. § 20-183.30 defines a law-enforcement purpose to include criminal investigations, arrests/prosecutions, post-conviction confinement or supervision, apprehending someone with an outstanding felony warrant, locating a missing/endangered person, and locating a lost or stolen vehicle. G.S. § 20-183.31 states that ALPR data obtained under the Article may not be used for traffic-violation enforcement.

A particularly strong practice is to require users to select or enter a search justification and a case number for each search.

7. Establish Explicit Prohibited Uses

A policy should expressly prohibit:

Personal searches	Searches based on protected characteristics
Searches for family or friends	Traffic enforcement per G.S. § 20-183.31
Searches based on curiosity	Using ALPR as the sole basis for enforcement action
Searches for political purposes	Sharing information with unauthorized persons

Searches unrelated to a criminal investigation	Downloading data to unauthorized devices
Circumventing system audit controls	Altering or deleting audit records

Personnel with access to ALPR databases should be notified of the consequences of misuse prior to accessing the system. Suspected misuse should be promptly investigated. Misuse can result in disciplinary action and, where applicable, criminal consequences. North Carolina law provides that unauthorized obtaining, accessing, preserving, or disclosing ALPR data can constitute a Class 1 misdemeanor, pursuant to G.S. § 20-183.33.

8. Audit the system routinely

Agencies should conduct regular reviews/audits. This review may be conducted weekly, monthly, or quarterly and should be specified in the agency's policy. Agencies should identify who is responsible for conducting the reviews. A review may require questions to be asked of an officer who conducts searches and/or the supervisor to determine the officer's work schedule, case assignments, and other factors that may help determine whether searches are valid or unjustified. In some instances, additional investigation may be warranted as determined by agency command staff.

Parameters which may be reviewed include identification of:

Excessive searches	Searches involving employees, family members, acquaintances, etc.
Searches without case/event numbers	Unusually broad geographic searches
Repeated searches on the same plate	Searches inconsistent with employee's assignment
Searches outside normal duties	Searches of the same plate over a long timeframe
Searches outside of work hours	Searches with multiple case numbers, but the same plate
Large volume searches	Exclusive external network searches

<u>Annual formal audit</u>

G.S. § 20-183.31 requires annual or more frequent auditing and reporting of ALPR use and effectiveness to the agency head. Audit records should be maintained according to the appropriate document retention schedule.

A formal audit should include the following parameters:

User activity	Hot-list accuracy
Search justification	False-alert rates
Data retention	System effectiveness
Sharing	Vendor compliance
Security	Complaints
Training compliance	Misuse incidents

The audit should include a review of which employees should maintain access to the system based on their role/assignment, including a review of account inactivity.

9. Establish strong hot-list governance

Hot lists are databases of license plate numbers and related vehicle information that are of interest to law enforcement. When an ALPR camera captures a vehicle's plate, the system can instantly compare it against a hot list. If there's a match, the system can trigger a real-time alert to investigators. There are two types of hot lists.

1) Automatic matches and alerts: ALPR systems compare scanned plates against SBI maintained National Crime Information Center (NCIC) databases of stolen vehicles, stolen plates, vehicles used in felonies and misdemeanors, carjackings, wanted persons, missing persons including juveniles, AMBER alerts, sex offenders, and protection orders. If there is a "hit" to one of these databases, officers receive an alert within seconds to allow them to locate the vehicle. This often leads to apprehension of a suspect, recovery of a stolen vehicle, recovery of a missing or endangered victim, and/or recovery of evidence from a crime (such as a handgun used in a homicide).
2) Manual hot list: Officers can set up a manual hot list of license plate numbers of suspects in their investigations so that they receive an alert when one of those vehicles' license plates is scanned by an ALPR.

It is considered misuse for an officer to include license plates on their manual hot list for personal reasons and/or out of curiosity. There must be a legitimate criminal investigative reason for a license plate to be included on a manual hot list. Agencies may consider requiring supervisor approval for licenses plates to be added to a hot list.

Manual hot lists should be reviewed regularly to determine if data needs to be kept longer based on an individual investigation. The Agency's policy should designate who will conduct this review. Removal should be automatic upon expiration. A vehicle should not remain on a hot list indefinitely.

Agencies may restrict which employees can add vehicles to a manual hot list to supervisors and/or detectives. Agencies may wish to institute an approval process for a vehicle to be added to a hot list. The approval process may include the officer sending an email to a supervisor or detective with a summary of the vehicle to be added, the reason for it to be added, the case number, and any other relevant information.

Every hot-list record should have:

Source	Entering agency/person
Date entered	Expiration/review date
Reason	Responsible owner
Case/event number	Verification status

10. Have written rules for interagency data sharing

Agencies should establish a formal data-sharing framework. G.S. § 20-183.31 states that data obtained by ALPRs shall be obtained, accessed, preserved, or disclosed only for law enforcement purposes. G.S. § 20-183.32 states that captured plate data shall not be disclosed except to a criminal justice officer for a legitimate law enforcement purpose pursuant to a written request. Furthermore, it states that captured plate data is confidential, not a public record, and shall not be sold for any purpose. Agencies should not share data with a non-law-enforcement agency.

Before sharing data, determine:

Who may receive data	Security requirements
What constitutes a legitimate law enforcement purpose	Restrictions on redisclosure
What request documentation is required	Audit requirements
Whether the receiving agency must have an ALPR policy	Vendor/cloud sharing
Retention requirements	Interstate sharing

11. Carefully govern vendor data

An agency's contract with the ALPR vendor(s) should address:

Data ownership	Breach notification
Data location	Audit rights
Encryption	System availability
Authentication	Incident response
CJIS/security requirements, where applicable	Data sharing
Vendor employee access	AI/analytics features
Subcontractors	Secondary use of agency data
Data retention	Sale or commercialization of data
Data deletion	Contract termination
Backup deletion	Data return/destruction

Agencies should avoid contracts that allow a vendor to use law-enforcement ALPR data for commercial analytics, marketing, profiling, or unrelated product development without explicit authorization.

12. Protect ALPR data like sensitive criminal justice information

Due to the sensitivity of ALPR data, security controls should include:

Unique user credentials	Administrative access controls
Strong authentication	Network segmentation where appropriate
Multi-factor authentication, where feasible	Backup controls
Strong password requirements	Security monitoring
No shared accounts	Documented incident response
Role-based access	Prompt termination of departing employees' access
Encryption in transit and at rest	Vendor security assessments
Detailed audit logs	Mobile device security
Automated account deactivation	Automatic session timeouts

Agency email addresses and agency cell phone numbers should be used for multi-factor authentication, so employees can no longer access the system after they leave the agency.

13. Establish strong training requirements

Users must be trained prior to being granted access to ALPR databases. Initial training for users should include:

ALPR purpose	Hot lists
Agency policy	Data retention
Legal authority	Data sharing
Constitutional considerations	Security
Investigative uses	Privacy
Authorized/prohibited uses	Misuse scenarios
Alert/hit verification	Audit/accountability
Historical searches	Disciplinary consequences
Search documentation	

Refresher training should be conducted before granting access and at least annually thereafter, and whenever there is a substantial policy, legal, or system change.

Supervisor training should include additional instruction on:

Reviewing searches	Investigative documentation
Identifying misuse	Preservation requests
Reviewing audit reports	Data-sharing requirements

14. Establish Accuracy and Quality Controls

Agencies should periodically evaluate:

Plate reading accuracy	Optical character recognition (OCR) accuracy
False positive rate	Alert accuracy
Camera positioning	Database freshness
Lighting	Vehicle description accuracy
Weather impacts	Camera uptime
Image quality	

G.S. § 20-183.31 requires agencies to maintain maintenance and calibration schedules and records. Agencies should maintain a formal ALPR maintenance/calibration log.

15. Require frequent updates

G.S. § 20-183.32 requires agencies operating ALPR systems to update the system from the databases specified in their policy every 24 hours when updates are available, or as soon as practicable after they become available.

Policies should therefore identify:

Authorized databases	Error correction procedures
Database owners	Procedures for removing invalid records
Update frequency	Data-sharing requirements
Update responsibility	