GO 2-57: Flock Camera Alert (ALPR) & Response Procedures

EFFECTIVE DATE: 07/01/23
REVIEW/REVISED DATE: 03/04/26
NEXT REVIEW DATE:
AMMENDMENTS/SUPERCEEDS:
APPROVED BY: W.T. JARRATT JR., SHERIFF

Note: This general order is for internal use only and does not enlarge officer's civil or criminal liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this directive, if proven, can only form the basis for a complaint by this department and then only in a non-judicial administrative setting.

I. PUPOSE

The purpose of this policy is to develop a standard operating procedure for the usage of the Flock camera system as well as handling alerts that are generated by the system.

II. POLICY

It is the policy of this office that alerts of the Flock camera system are monitored twenty-four hours a day. This allows law enforcement officers to be dispatched to all flock alarms as soon as possible. This policy also will build a streamline process for the receiving, processing, dispatching and response to all flock alerts.

III. PROCEDURE

A. Access

i. Access will be granted to all law enforcement certified staff as well as all communications center staff.

ii. Any other personnel inside or outside of the department who request access, must be approved by the sheriff or his designee.

B. Usage

i. Operation of any ALPR system is only permitted by authorized users for official law enforcement purposes only as permitted by Virginia Code § 2.2-5517. No user may utilize or authorize the use of the equipment, images, or database records for any other reason and must complete a training session prior to the use of the ALPR equipment or related systems. ALPR systems are used to identify vehicles, not people. Misuse of the ALPR systems or data may result in disciplinary action and/or criminal and civil penalties.

ii. No one shall utilize ALPR systems for the purpose of interfering with individuals engaged in lawful activities or tracking individuals on the basis of lawfully protected speech.

iii. Users are required to have reasonable articulable suspicion for conducting a query or search of an ALPR system. State law permits searches of ALPR systems for the following reasons:

1. As part of a criminal investigation into the violation of the Code of Virginia or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed (no federal investigations); or

2. As part of an active investigation into a missing or endangered person (including, where needed in order to determine whether to issue an alert for such a person) or a person associated with human trafficking; or,

3. To receive notifications for a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle or a stolen license plate.

iv. Users are prohibited from querying or downloading system data unless such data is related to one of the purposes outlined in Section C above.

v. All information necessary for the creation of an audit trail shall be entered in order to query system data.

1. Users who conduct queries or searches in an ALPR system must provide the search reason. At a minimum, searches must include the offense type and the reasonable articulable suspicion for the search. (e.g., Stolen Auto – Victim reported vehicle stolen.)

2. Additionally, a case number or call for service number associated with the search will be required. An official record number (e.g., CAD Event ID or a Report Number) that is associated with each search or query in an ALPR system.

3. Generic reasons (e.g., investigation, stolen, drugs, CFS) are prohibited.

4. There are instances where a search may be conducted upon receiving a BOLO by radio from another jurisdiction. In these cases, the reason field should include the jurisdiction, BOLO, and call type (e.g., EPD BOLO Missing Person, BCSO BOLO Pursuit) and will require a report or CAD #. This may be achieved by contacting that jurisdiction's Communications center and obtain their report number or CAD event ID.

vi. The use of and activity in ALPR systems by users will be logged and subject to periodic audits occurring at least once every 30 days.

C. Alerts & Hot Lists

A. Alerts will be monitored by staff of the E-911 Communications Center twenty-four hours a day. This will be monitored via the web-based Flock interface.

B. An 'alert', 'hit', or 'notification' resulting from an ALPR system shall not constitute reasonable articulable suspicion to stop or effect an arrest. Prior to stopping a vehicle based on a notification, users are required to:

1. Develop independent reasonable articulable suspicion to make a traffic stop; **or**,
2. Confirm the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification.
    a This confirmation procedure shall be an independent comparison of the ALPR system alert and the corresponding hot list notification.

    b Law enforcement officers are encouraged to use radio communication to verify the ALPR system alert.

3. When the ALPR system matches an alpha-numeric string from a hot list, a visual and/or audible ‘alert’ will be prompted. The user shall confirm a positive ‘hit’ prior to any enforcement action being taken.

4. After confirming the plate and ‘hit’ status, a traffic stop may be conducted

5. Mobile ALPR operators shall select “Action Taken”, “No Action Taken” or “False Hit” on the ALPR portal website after their investigation.

6. ALPR users shall ensure entries into NCIC/VCIN hotlists are removed or make notifications to the originating jurisdiction based on investigative efforts within 24 hours, or as soon as practical, after such updates become available. For example, if a stolen vehicle is recovered, the VCIN record will need to be updated to reflect the vehicle is no longer stolen prompting VCIN removal. The Virginia State Police distributes updated NCIC hot lists four times daily.

7. Access to make changes to the State Police Hot List will not be permitted by anyone other than the administrators of the ALPR systems, at the direction of the vendor or the Virginia State Police, to troubleshoot or resolve problems. No other users will attempt to make any changes to the State Police Hot List.

8. Authorized users are permitted to create ALPR system custom hot lists provided that the license plate or vehicle description is entered for a permissible use outlined above in I. C. The creator of the custom hot list must set an expiry date no longer than 90 days from the date of entry and is responsible for maintaining up-to-date records as to the reason the license plate was entered.

    a. Custom Hotlist users are Patrol Lieutenants, Investigations Division and Command Staff

9. Manually entered license plate lists shall contain at a minimum:
    a. Supporting information regarding why a particular license plate is on a specific hot list.
    b. Vehicle description (year, make, model, and color)
    c. Legal reason for entry
    d. Valid report number. In event there is no case number, the CAD event ID must be used

D. Data Storage & Retention

A. ALPR collected data, storage and retention requirements are governed by the Virginia Code 2.2-5517

1. System data collected by ALPR fixed and portable systems are maintained by the Division in its original read format for 21 days. Internal data storage settings of Division mobile ALPR systems shall be set to purge data within 21 days of its collection.

2. Audit trail data shall be purged after two years of the date of its capture and rendered non- recoverable in accordance with Virginia Code § 2.2-5517, section E.

B. ALPR system and audit trail data is owned by the Division.

C. The Division may retain ALPR data that relates to a specific, on-going, criminal investigation, prosecution, or civil action until (1) the investigation ends without charges; or (2) a final disposition is made in any criminal or civil matter related to the data including any direct appeals or writs of habeas corpus (refer to Virginia State Code § 2.2-5517

E. Data Sharing & Dissemination

A. Security procedures to protect the ALPR system, system data, and audit trail data from unauthorized access, destruction, use, modification or disclosure are in place for Division ALPRs. ALPR data is categorized as 'for official use only.' All collected data will be maintained on a server that is not connected to, or shared with, other law enforcement databases. The server will be able to provide an inquiry tool, history tracking, and reporting protocols for the entire ALPR systems. Ensuring ALPR data remains secure builds public confidence in this technology. Unauthorized dissemination of the data is prohibited.

B. Access to ALPR data is controlled by multifactor authentication on all Division computers, including mobile data terminals (MDT). Individual usernames and passwords are required

C. ALPR system and audit trail data is not subject to release under the Freedom of Information Act (FOIA).

D. The Division may share ALPR system data with: Another law enforcement agency as defined by Virginia Code § 2.2-5517 for one of the permissible use reasons outlined above in section.,

1. A Commonwealth's Attorney for one of the permissible reasons outlined above or for complying with discovery or a court order in a criminal proceeding; defendant or defense counsel for purposes of complying with discovery or a court order in a criminal proceeding

2. A vendor for maintenance or quality assurance purposes, and/or

3. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding warrant.

4. The department will not share or sell system data or audit trail data to any other state, federal, private, or commercial entity.

F. Operator/User Training

A. All users must receive standardized training prior to using or accessing the ALPR systems.

B. ALPR standardized training shall include:

1. The purpose of the ALPR policy,

2. Appropriate reasons for the use of ALPR data,

3. Appropriate reasons for the searching of ALPR data,

4. Verification of hits/alerts/notifications from an ALPR system, and

5. Security and dissemination of ALPR data.

C. Training and updates concerning ALPR systems shall be coordinated through the Administrative Captain & Captain of Investigations

D. The Administrative Captain will be responsible for the maintenance of all training records associated with the ALPR program.

G. ALPR Audits

A. The Captain of Investigations will be responsible for audits of Division ALPR systems and will conduct an audit at least once every 30 days. The documented audit is designed to ensure proper use of the ALPR systems to cover the following use areas: system users, queries conducted, and sharing with other agencies. ALPR administrators may download audit trail data for the purpose of generating audit reports.

H. Definitions

A. ALPR System – A system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data.

B. ALPR System Data – All forms of data collected or generated by an ALPR system, including images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted.

C. ALPR Administrators – The Administrative Captain & Captain of Investigations shall be responsible for the management and administration of the Division ALPR systems.

D. ALPR Read – Digital images of license plates, vehicles and associated data (e.g., date, time, and geographic coordinates associated with the image capture).

E. ALPR Users – Authorized members utilizing the ALPR portal websites to access information and/or conduct search functions for criminal justice purposes.

F. Audit Trail Data – All forms of data collected or generated by an ALPR system for purposes of producing an audit trail.

G. Fixed ALPR system - ALPR cameras that are affixed to a structure, such as a pole or a traffic control device.

H. Hit/Alert/Notification – An alert from an ALPR system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the ALPR system for comparison purposes.

I. Hot Lists – License plate numbers and letters of stolen vehicles, vehicles owned by persons of interest and vehicles associated with AMBER alerts that are regularly added to hot lists circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle

information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER alerts and Department of Homeland Security watch lists. Law enforcement agencies can also interface their own, locally compiled hot lists to the ALPR system. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if a vehicle license plate of interest is read by the ALPR system.

J. Portable ALPR System – ALPR systems that are self-contained, portable devices that may be relocated, as needed, to address public safety/criminal concerns.

K. Mobile ALPR Maintainers – Designated individuals in specified units that will have the ability to enter license plates into designated lists and manage data retention for the mobile ALPR system.

L. Mobile ALPR Operators – A user properly trained in the physical use of the Division's mobile ALPR system.

M. Mobile ALPR System – ALPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

N. Private Entity ALPR system - A private entity may be, but not limited to, homeowner's associations, gated communities, shopping malls, other business establishments, or places of worship. These entities often have information sharing agreements with law-enforcement agencies.

O. Person Associated with Human Trafficking – A person who is either a suspected victim or an alleged perpetrator of either commercial sex trafficking or labor trafficking.

P. Query – A search of ALPR system data based on information entered by the user, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the ALPR system.

I. Communications Center Responsibility

A. The E-911 Communications Center upon receiving a Flock alert shall review the alert immediately and generate a call for service for a law enforcement response.

B. Create a CFS using the location where the flock alarm was received. Flock cameras have been assigned a 911 address and can be found in CAD using B/FLOCK.

1. The address should remain as the Flock cameras address. When a deputy makes contact with a person or vehicle, they will advise the Communications Center via radio and it will be updated as a location change in CAD.

C. All flock alerts will use the nature code "Flock".

D. The notes of the call should reflect what the alert was and all pertinent information from the alert to include:
    a. Type of alert (Amber, stolen vehicle, Missing Person, etc.)
    b. Vehicle Type (Make, Model, Color and Tag)

E. The call should be immediately dispatched to the CAD recommended unit via radio.

F. All flock alerts must be confirmed in VCIN/NCIC.
    1. Vehicles should be queried by VIN or license plate
    2. Persons should be queried only by name and date of birth in Virginia

G. Once the Flock Alert is dispatched, it must confirm the alert via VCIN/NCIC by querying the information provided in the Flock Alert. Alert all responding units it has been confirmed in VCIN/NCIC & document it in the CFS.

H. Once the vehicle has been stopped and/or person(s) have been detained, begin the VCIN/NCIC process of sending a HIT to the entering jurisdiction. Hits should not be sent until the vehicle is stopped and proper driver and occupant identification made

J. Law Enforcement Responsibilities

A. If you receive an alert but have not been notified by the E-911 Communications Center, confirm with them that they received the alert.

B. All law enforcement responses will be a “Code 2” response unless a supervisor deems that a “Code 1” response is needed.

C. Law Enforcement officers must ensure that the alert has been queried and confirmed through VCIN/NCIC by dispatch before conducting a vehicle stop. Once has been confirmed by dispatch to be positive, the stop can be conducted unless you have found reasonable suspicion to conduct the stop beforehand.

    1. A flock alert alone, **IS NOT** grounds to stop a vehicle or detain a person. ALL alerts **shall** be confirmed by dispatch prior to making a stop or detaining a person.

D. Once the vehicle has been stopped and or person(s) have been detained and identified, the Communications Center will then begin the VCIN/NCIC process of sending a HIT the entering jurisdiction.

E. When patrol officers of this department take a report for a stolen vehicle, s/he shall make contact with one of the listed employees who manage the Hot List to enter the vehicle stolen into the Flock system immediately. The Flock system syncs with NCIC which is every 6 hours. This will allow us to receive notifications as soon as they pass a Flock Camera. Once the vehicle is located, the vehicle must be removed from the Hot List immediately.

F. A report must be completed for each Flock alert that patrol officers make an arrest from and also use offense code “Flock Arrest”.

G. In cases where no arrest is made the primary officer must complete a Flock Contact Field Contact and add all names and vehicles to the field contact. Also,

the notes box must contain detailed notes of the stop, interactions and disposition of the call.