INDEPENDENT AUDITOR'S REPORT

St. Cloud Police Department

APRIL 29TH, 2026

RAMPART AUDIT LLC

Automated License Plate Reader Audit Report

Dear Chief Oxton:

We have audited St. Cloud Police Department's (SCPD) Automated License Plate Reader (ALPR) program for the two-year period ended 2/28/2026.

The purpose of this audit is to evaluate SCPD's compliance with Minn. Stat. §13.824, which sets forth requirements and prohibitions governing the use of ALPRs and the collection, use, management and destruction of ALPR data, and Minn. Stat. §626.8472, which mandates that the chief law enforcement officer (CLEO) of any agency that maintains an ALPR system in Minnesota establish and enforce a written policy governing the use of the system, and also sets forth minimum requirements for the ALPR system policy.

Minn. Stat. §13.824 Subd. 6 requires that an agency shall arrange for an independent, biennial audit of its ALPR records "to determine whether data currently in the records are classified, how they are used, whether they are destroyed as required… and to verify compliance with [Minn. Stat. §13.824] Subdivision 7," which governs authorization to access data. This program and its associated data are the responsibility of the St. Cloud Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On March 5, 2026, Rampart Audit, LLC (Rampart) met with Lieutenants Jason Burke, Justin Day and Alec Elness, who provided information about SCPD's ALPR program and facilitated access to SCPD ALPR data by running reports and retrieving sample data at the direction of Rampart. Please note that all ALPR data access undertaken for the purpose of this audit occurred between the hours of 12:45 PM and 2:00 PM on 3/05/2026 and was logged in the ALPR system with a reason code of "Rampart ALPR audit." No direct system access was granted to the auditors, nor was any data downloaded by the auditors.

ALPR PROGRAM

Lieutenant Burke advised us that SCPD operates both mobile and stationary ALPRs. The stationary ALPRs were deployed first, on March 4, 2024, and the mobile ALPRs were subsequently activated on July 12, 2024.

St. Cloud Police Department employs the Axon Fleet ALPR system, which utilizes optical character recognition (OCR) technology built into the existing in-car cameras installed in SCPD squads. The Axon

ALPR system integrates with the squad's mobile data terminal (MDT), and is normally active whenever the camera is powered on. At the time of our audit, SCPD had deployed approximately 39 of its 40 Axon Fleet ALPRs. We noted that the number of mobile ALPRs deployed may vary as squads are retired from service and replaced.

The Axon ALPR system compares each scanned license plate to three databases. The Minnesota License Plate Data File contains a limited version of the Minnesota DVS database, which includes a list of those vehicles registered to individuals whose driving status is identified as suspended, revoked, canceled or disqualified. This file also contains FBI NCIC data related to stolen and felony vehicles, wanted persons and attempts to locate. The National Center for Missing and Exploited Children (NCMEC) database contains Amber Alert data. The Manual Hot List File contains a list of license plates related to active investigations which have not been entered in the Minnesota License Plate Data file. While these condensed databases may be updated multiple times per day, they are not considered "live" data.

The Axon system integrates with the squad's mobile data terminal (MDT), and is normally active whenever the camera is powered on. The ALPR software runs in the background and the vast majority of license plate reads require no action on the part of the officer. When the ALPR identifies a possible match to a license plate listed in one of the databases listed above, or "hit," it triggers an audible alert and activates a window on the MDT to display information about the alert, including the nature of the hit and two images: a close-up of the license plate, and a wide-angle view that shows portions of the vehicle and the area immediately surrounding the vehicle. The screen will remain active until the officer provides a response to the hit.

In most instances, the officer is able to dismiss the hit alert without taking further action. Common reasons for hit dismissals include scans of parked vehicles indicating that the registered owner lacks a valid driving status, state mismatches and misread plate numbers. Officers will also dismiss alerts that result from scans that occur while responding to higher priority calls. When an alert is not dismissed, officers are required to confirm the hit information through the appropriate live database (DVS or NCIC) before taking enforcement action.

Data from mobile ALPR scans, including hit data, upload wirelessly to Axon's secure cloud storage service, Evidence.com. MDPS retains mobile ALPR data for 60 days, after which it is permanently deleted. ALPR data is retained beyond 60 days only when classified as active investigatory data, or when so requested in writing by an individual who is the subject of a criminal investigation and who identifies the data as potential exculpatory evidence. Any ALPR data to be retained beyond 60 days is exported through a manual process to a separate Evidence.com database and is retained as evidence until manually purged.

St. Cloud Police Department also employs a total of five (5) Flock Safety stationary ALPRs. These cameras are positioned at two (2) intersections within the city and operate continuously. The Flock system also utilizes OCR technology to scan license plates and determine the plate number, and compares the scanned license plate to the same three databases.

When a stationary ALPR identifies a possible match to a license plate listed in one of those databases, it is able to generate alerts via text, email or the Flock Safety cellular phone application. At the time of our audit, SCPD advised us that these alerts are being directed only to those officers who are logged into the Flock portal at the time the alert is generated.

Data from stationary ALPR scans, including hit data, upload wirelessly to Flocksafety.com, which utilizes Amazon Web Service's GovCloud for secure CJIS storage. By default, Flock retains ALPR data for 30 days, after which it is permanently deleted. Stationary ALPR data are retained beyond 30 days only when classified as active investigatory data, or when so requested in writing by an individual who is the subject of a criminal investigation and who identifies the data as potential exculpatory evidence. Any stationary ALPR data to be retained beyond the 30-day default retention period are exported through a manual process to Axon's Evidence.com, where it is retained as evidence until manually purged.

At the time of our audit, SCPD retained records of 1,053,902 mobile ALPR reads, which included 7,603 hits during the preceding 60 days. SCPD also retained 94,035 stationary ALPR reads, which included 5,304 hits, during the preceding 30 days.

ALPR POLICY

As noted above, Minn. Stat. §626.8472 states:

> The chief law enforcement officer of every state and local law enforcement agency that maintains an automated license plate reader shall establish and enforce a written policy governing use of the reader. Use of an automated license plate reader without adoption of a written policy under this section is prohibited. At a minimum, the policies and procedures must incorporate the requirements of section 13.824, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Rampart reviewed a copy of St. Cloud Police Department's ALPR policy and compared it to the requirements and prohibitions contained in Minn. Stat. §13.824. In our opinion, SCPD's ALPR policy addresses all of the mandatory elements identified in the statute, including the employee discipline standards for unauthorized access to ALPR data. A copy of the policy has been attached to this report as Appendix A.

DATA COLLECTION

Minn. Stat. §13.824 Subd. 2 limits ALPR data collection to the following elements:

1. License plate numbers;
2. Date, time and location data on vehicles; and
3. Pictures of license plates, vehicles and areas surrounding the vehicles.

Rampart selected a random sample of license plate scans from both the Axon and Flock systems. We reviewed the sample data against the list of permitted data elements above. We did not note any exceptions.

Axon's ALPR system employs artificial intelligence (AI) to analyze the photos and develop what it terms Vehicle Attribute Recognition (VAR) data. This includes details such as the vehicle's make, model, body style and color, as well as the license plate's state of issuance. Each element is given a probability score, Axon's estimate as to the reliability of its analysis. This data is retained along with the §13.824 Subd. 2 data. We noted that these VAR elements are not "collected," but rather are the product of AI analysis that is applied to the photographs collected under Subd. 2.

Similar to the Axon system, Flock's ALPR system employs artificial intelligence (AI) to analyze the photos and develop what it terms Vehicle Fingerprint (VF) data. This includes details such as the vehicle's make, model, body style and color; unique elements such as roof racks, stickers or damage; as well as the license plate's state of issuance. In addition, Flock Safety's website describes its system as possessing at least limited ability to identify vehicles based on VF elements, even in the absence of a license plate. As with the Axon VAR data, we noted that these VF elements are not "collected," but rather are the product of AI analysis that is applied to the photographs collected under Subd. 2.

Both ALPR systems also record the identity of the camera conducting each read, as well as any response to a hit entered by a user. We noted that these details are not data collected by the license plate reader itself, but rather could be deemed metadata – that is, additional data about the ALPR read or hit data that are necessary for auditing and classification purposes.

DATA CLASSIFICATION

Minn. Stat. §13.824 Subd. 2(b) states:

> All data collected by an automated license plate reader are private data on individuals or nonpublic data unless the data are public under section 13.82, subdivision 2, 3, or 6, or are active criminal investigative data under section 13.82, subdivision 7.

While SCPD's ALPR policy does not explicitly state this, the access requirements and controls documented in the policy are appropriate for private or nonpublic data.

Lt. Burke advised us that SCPD has not received any requests for ALPR data from members of the public or from other law enforcement agencies. In order to obtain access to SCPD data, a requesting agency would be required to submit a written request that includes the following:

- The name of the agency.
- The name of the person requesting the data.
- The intended purpose of the data.
- A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.

- A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

Once received, the request is reviewed by a supervisor. If approved, the supervisor creates an agency assist case in SCPD's RMS and documents the information listed above. In addition, SCPD retains a copy of the written request.

When fulfilling a request from another agency, we recommend adding a written reminder of the receiving agency's data privacy responsibilities to the email used to provide the requested data.

PUBLIC LOG OF USE

Minn. Stat. §13.824 Subd. 5(a) requires that "[a] law enforcement agency that installs or uses an automated license plate reader must maintain a public log of its use…" and requires that the agency maintain the following data as part of the log:

1. Specific times of the day that the reader actively collected data;
2. The aggregate number of vehicles or license plates on which data were collected for each period of active use;
3. A list of all state and federal databases with which the data were compared, unless the existence of the database itself is not public;
4. For each period of active use, the number of vehicles or license plates in each of the following categories:
    a. The vehicle or license plate has been stolen;
    b. There is a warrant for the arrest of the owner of the vehicle;
    c. The owner of the vehicle has a suspended or revoked driver's license or similar category; or,
    d. The data are active investigatory data
5. For fixed or stationary readers, the location at which the reader is installed and used and actively collected data.

A complete list of St. Cloud Police Department' stationary ALPRs is available on the Minnesota Bureau of Criminal Apprehension website. All of the stationary ALPRs are operational at all times. The Flock system captures the remaining elements from the list above.

The Axon system also captures the required data elements; however, as of the date of our audit, it was not clear whether Axon offered a pre-programmed report capable of providing information about the specific times of the day that each ALPR actively collected data. We noted that this requirement might require clarification from the legislature as to whether the log would need to list the time of each individual scan, or whether a summary report listing the times of the first and last scan of each day would suffice.

We noted that the statute provides limited guidance to the agency for creating the public log of use. While it identifies the required data elements, it doesn't specify how frequently the log should be

produced or how long it should be retained. We did note that the General Records Retention Schedule for Minnesota Cities recommends that an ALPR public log of use be retained for two years.

As part of the audit, Rampart reviewed SCPD's "transparency portal" for each system, which provides publicly-accessible information similar to that which is required by the public log of use, as well as additional information about how ALPR data is, and is not, used. While the transparency portal data does not satisfy all of the requirements specified for the public log of use, those remaining data elements are captured by the systems.

NOTIFICATION TO THE BCA OF THE LOCATION OF ANY FIXED/STATIONARY ALPRs

Minn. Stat. §13.824 Subd. 5(b) requires that:

> The law enforcement agency must maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary automated license plate readers or other surveillance devices with automated license plate reader capability used by the agency. The agency's list must be accessible to the public, unless the agency determines that the data are security information as provided in section 13.37, subdivision 2. A determination that these data are security information is subject to in-camera judicial review as provided in section 13.08, subdivision 4.

As noted above, St. Cloud Police Department had deployed five (5) stationary ALPRs at the time of our audit. As part of this audit, Lt. Burke furnished a list of stationary ALPR locations. Rampart compared this list to the list published on the Minnesota Bureau of Criminal Apprehension website and verified that both were identical.

We noted that while both state statute and SCPD's ALPR policy require that the agency maintain a list of previous locations, the statute does not provide guidance as to how long the list of previous locations must be maintained. In the absence of authoritative guidance, Rampart recommends that such data be maintained for two years. Lt. Burke advised us that none of the agency's ALPRs have been moved since their initial placement. We recommend retaining copies of the emails used to notify the BCA of the initial placement, as well as copies of any emails documenting the future movement of ALPRs, to ensure historical location information is available for at least two years.

ALPR DATA ACCESS CONTROLS

Minn. Stat. §13.824 Subd. 7(c) requires that:

> The ability of authorized individuals to enter, update, or access automated license plate reader data must be limited through the use of role-based access that corresponds to the official duties or training level of the individual and the statutory authorization that grants access for that purpose. All queries and responses, and all actions in which data are entered, updated,

> accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public, to the extent that the data are not otherwise classified by law.

Lt. Burke furnished a list of authorized internal users of ALPR data as part of this audit, and further advised us that access to the ALPR system is role-based, as required by statute. All officers have access to search and respond to hits, while hotlist update access is limited to supervisors and SCPD's four super-users.

Access is granted to new SCPD officers as part of the field training process, which includes a requirement that the officer read and sign off on the SCPD ALPR policy.

SCPD personnel advised us that the Flock Systems data sharing function is turned off; consequently, outside agencies can obtain SCPD ALPR data only through the written request procedure outlined earlier in this report.

ALPR DATA AUDIT TRAIL

Lt. Burke ran an Audit Trail Report for each ALPR system. While both systems were able to produce an audit log, we noted that the Axon audit trail is currently unrefined and difficult to read. The log we reviewed consisted of an Excel download with many of the data elements for each entry concatenated into a long alphanumeric string. This is consistent with Axon logs we have reviewed as part of other audits and appears to be a limitation of the system. We encouraged SCPD to request that Axon develop a more user-friendly audit trail report.

ALPR DATA DESTRUCTION

Minn. Stat. §13.824 Subd. 3(a) requires that ALPR data be destroyed no later than 60 days from the date of collection, subject to certain exceptions described earlier in this report. While St. Cloud Police Department's policy specifies a 60-day retention policy for ALPR data, and that setting is applied to data in the Axon Evidence.com cloud storage site, Flock Safety limits data retention to 30 days. Settings in the storage sites of both systems automatically delete permanently any data contained in the respective ALPR database once it reaches the corresponding data retention limit. As discussed earlier in this report, by statute ALPR data can be retained beyond 60 days only when identified as active investigatory data, or when requested in writing as potential exculpatory evidence. In such cases, the ALPR data is then manually exported to a separate evidentiary database within Evidence.com.

As part of the audit, Lt. Burke ran a report to list any retained ALPR data within the Axon ALPR database that was more than 60 days old, as well as a second report to list any retained ALPR data within the Flock ALPR database that was more than 30 days old. Both reports showed no retained data beyond the corresponding retention period.

INTERNAL CONTROL RECOMMENDATIONS

Lt. Burke advised us that all officers have access to respond to hits and conduct searches in the ALPR systems, while hotlist updates are limited to supervisors. In addition, there are four super-users with full access rights. As noted earlier in this report, ALPR access is granted as part of the field training process after the officer signs off on the ALPR policy and completes training on its use and requirements.

Users conducting searches in the Axon system are required to provide both the associated case number and a search reason, while searches conducted in the Flock system require a case number, search reason and offense type.

Lt. Burke advised us that access is logged and reviewable in the audit trails of both ALPR systems; however, there are currently no internal audit requirements. We recommend that a minimum of two administrators or supervisors conduct periodic reviews or internal audits to review data access, and document such reviews with a reason code of “admin audit” or a similar meaningful description. Doing so will avoid requiring an employee to review his or her own activity.

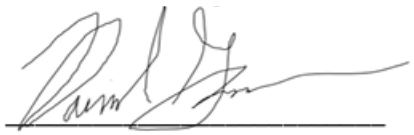
We recommend conducting the following internal audit tests, subject to the limitations of the audit trail report of each ALPR system:

1. Review any license plates that are searched multiple times.
2. Conduct random reconciliations of license plate searches to the case number listed in the audit log as the reason for the search, to ensure the search was appropriate.

We recommend ensuring that audit log data are retained for a minimum of thirty (30) months, to accommodate biennial audits.

AUDIT RESULTS

Based on our review of St. Cloud Police Department’s ALPR policy and operations, as well as the on-site tests conducted and data reviewed as part of our audit, it is our opinion that SCPD’s ALPR program is compliant with the requirements of Minn. Stat. §13.824 and §626.8472



Rampart Audit, LLC

4/29/2026

APPENDIX A:

ST. CLOUD POLICE DEPARTMENT
Law Enforcement
Policies and Procedures

Subject: Automated License Plate Readers	Policy Number: 305
Issue Date: 02-02-15	Revision Date: 02-02-15; 08-05-15; 07-16-24
Approval Authority - Title and Signature: Jeffrey Oxton, Chief of Police	
Reviewed By: Adam Meierding, Commander	Reviewed Date: 02-02-15; 08-05-15; 07-16-24

POLICY

It is the policy of the St. Cloud Police Department to utilize and operate automated license plate reader technology (ALPR). ALPR technology, also known as License Plate Recognition (LPR), provides automated detection of license plates.

PROCEDURE

ALPRs are used by law enforcement to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons ALPRs may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

A. **Definitions:**

1. Automated License Plate Reader (ALPR): A device that uses infrared cameras to scan license plate data of moving and stationary vehicles. This data is then compared to a downloaded "hot list" to identify license plates associated with certain unlawful acts.
2. Hot List: A downloadable list of stolen vehicles and license plates, suspended or revoked licenses and registrations as well as any other unlawful activity information. This information is provided by the Minnesota Department of Public Safety's Driver and Vehicle Services (DVS) Division, National Crime Information Center (NCIC), and the Bureau of Criminal Apprehension (BCA).

3. Alert/Hit: An alert or hit is generated when the Automated License Plate Reader identifies license plates that have the possibility of matching information on the hot list.

B. **Administration of ALPR data:**

The Chief of Police or his/her designee will assign personnel under his/her command to administer the day-to-day operation of the ALPR equipment and data.

C. **ALPR Operation:**

Use of an ALPR is restricted to the purposes outlined below. Department personnel shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
2. An ALPR shall only be used for official and legitimate law enforcement business.
3. An ALPR may be used in conjunction with any patrol operation or official department investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.
4. ALPRs must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant.
5. An agency's case number or incident number shall be associated with a search of the ALPR data. In the case of an emergency, the complaint or incident type can be the factual basis for the access.
6. ALPRs will be primarily used to identify possible stolen plates and vehicles, suspended or revoked license holders, and vehicle registrations; however, license plate information may be entered manually in situations where exigency exists. A supervisor will have the ability to manually enter an alert if exigency exists or a search warrant is obtained. The reason for the exigency must be entered.
7. An alert, in and of itself, does not constitute probable cause or reasonable suspicion to initiate a traffic stop. All alerts must be confirmed by the officer and reasonable suspicion or probable cause must be established before conducting a traffic stop.
8. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings, and other major incidents.

9. If practical, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.
10. No ALPR operator may access MNJIS or NLETS data unless otherwise authorized to do so. ALPR operators must obtain clearance through the Bureau of Criminal Apprehension (BCA) prior to operating ALPR equipment or accessing ALPR data.

D. **Limitations of the ALPR:**

1. Because the ALPR is not connected to a "real-time" database, but rather a downloadable file, the data on the ALPR may be outdated. As such, it is imperative for officers to independently confirm all alerts before acting on an ALPR return.
2. The ALPR may generate a false-positive alert in certain instances, such as if another state's license plate number matches the numbers of a Minnesota license plate on the hot list.

E. **Procedures:**

1. Receiving an alert

a. When the ALPR detects a hot list entry, an audible alert and visual notification will be generated.
b. An alert on its own shall not be used as reasonable suspicion or probable cause for a traffic stop or enforcement contact. Contact with the vehicle and/or occupants may only be made after the alert is confirmed by matching the vehicle information with the hot list description and verifying information through appropriate means such as the Communications Center, DVS, CJIS, originating agency, etc.
c. If an officer issues a citation or makes an arrest based on an ALPR alert, the officer shall upload the alert into Evidence.com under the appropriate case number and save it as evidence. The officer shall complete data entry in the system in which the alert was generated.

F. **ALPR Data Collection and Retention**

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

1. Exculpatory evidence – Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.

2. Address Confidentiality Program – Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

G. **Log of Use**

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

1. Specific times of day that the ALPR collected data.
2. The aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal public databases with which the data were compared.
3. For each period of active use, the number of vehicles or license plates related to:

a. A vehicle or license plate that has been stolen.
b. A warrant for the arrest of the owner of the vehicle.
c. An owner with a suspended or revoked driver's license or similar category.
d. Active investigative data.

4. For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

H. **Accountability**

All saved data will be closely safeguarded and protected by both procedural and technological means. The St. Cloud Police Department will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

1. All ALPR data downloaded and in storage shall be accessible only through a login/password-protected

system capable of documenting all access of information by name, date and time.

2. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or office-related civil or administrative action.

3. Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.

4. Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).

5. All queries and responses, and all actions in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.

6. Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

I. Releasing ALPR Data

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

1. The agency makes a written request for the ALPR data that includes:

a. The name of the agency.
b. The name of the person requesting.
c. The intended purpose of obtaining the information.
d. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
e. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

2. The request is reviewed by a supervisor and must be approved before the request is fulfilled.

    a. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.
        2. The approved request is retained on file.

            a. The approving supervisor will start an assist agency case/incident number and document in comments, the agency that is requesting data, the requesting agency's case number, and the requesting officer.
            b. The approving sergeant will save the written request under the assist agency case number.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.