INDEPENDENT AUDITOR'S REPORT

Paul Bunyan Drug Taskforce c/o Beltrami County Sheriff's Office

NOVEMBER 28TH, 2025

RAMPART AUDIT LLC

Automated License Plate Reader Audit Report

Dear Sheriff Riggs:

We have audited the Paul Bunyan Drug Task Force's (PBDTF) Automated License Plate Reader (ALPR) program for the two-year period ended 10/23/2025. While the PBDTF is a multi-agency task force encompassing five counties, two cities and two Indian reservations, because PBDTF operates its ALPR program under the Beltrami County Sheriff's Office's (BCSO) Originating Agency Identifier (ORI), this report is being addressed to you as the chief law enforcement officer of BCSO.

The purpose of this audit is to evaluate PBDTF'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 Paul Bunyan Drug Task Force. Our responsibility is to express an opinion on the operations of this program based on our audit.

On October 23, 2025, Rampart Audit, LLC (Rampart) met with Commander David Hart, who provided information about PBDTF's ALPR program and facilitated access to PBDTF 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 2:30 PM and 4:30 PM on 10/23/2025 and was logged in the ALPR system with a reason code of "ALPR audit." No direct system access was granted to the auditors, nor was any data downloaded by the auditors.

ALPR PROGRAM

Commander Hart advised us that PBDTF's ALPR program began in May of 2023. As of the date of the audit, PBDTF has leased 13 stationary ALPRs, which have been deployed along key travel corridors throughout the task force's operational area. PBDTF does not currently employ mobile ALPRs. Commander Hart also advised us that the Flock Safety cellular phone application used by PBDTF agents is capable of scanning license plates; however, Minn. Stat. §13.824 Subd. 1(b) defines an automated license plate reader as "an electronic device mounted on a law enforcement vehicle or positioned in a

stationary location." In our opinion, a cellular phone using this software does not meet the definition of an ALPR.

The Paul Bunyan Drug Task Force employs the Flock Safety ALPR system, which utilizes optical character recognition (OCR) technology to scan license plates and determine the plate number. The Flock cameras compare 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 ALPR cameras are continuously active, with the exception of one camera that has experienced intermittent power issues. When the ALPR identifies a possible match to a license plate listed in one of the databases listed above, or "hit," it is able to generate alerts via text, email or the Flock Safety cellular phone application. PBDTF agents are able to select both the types of alerts for which they are notified and the notification method. Agents are also able to turn off notifications when they're off duty. The vast majority of license plate reads do not result in a "hit" or generate an alert. Of the license plate reads that do result in a "hit," the majority involve issues with the registered owner's driving status.

Because the PBDTF is an investigative agency, task force personnel do not monitor alerts related to driving status, and Commander Hart advised us that agents are not required to respond to alerts in the system. Agents primarily monitor alerts related to specific investigations, but are also able to notify the appropriate dispatch office when receiving Kops Alerts or other time-sensitive information that can then be forwarded to Patrol personnel.

Data from 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. 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 ALPR data to be retained beyond the 30-day default retention period are exported through a manual process to an independent virtual server maintained by Beltrami County's Information Technology department.

Commander Hart advised us that there have been recent discussions with two PBDTF member agencies, the Beltrami County Sheriff's Office and Bemidji Police Department, about sharing ALPR alerts directly with their patrol staff; however, this had not occurred at the time of our audit. Commander Hart subsequently advised us that any "hits" would likely by shared with Dispatch instead, and then could be relayed to patrol personnel.

At the time of our audit, PBDTF retained records of 1,225,448 ALPR reads, comprising 138,448 unique license plates, and 4,941 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 Paul Bunyan Drug Task Force's ALPR policy, which Commander Hart advised is actually a Beltrami County Sheriff's Office policy adopted by PBDTF, and compared it to the requirements and prohibitions contained in Minn. Stat. §13.824. In our opinion, PBDTF'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 ten license plate hits from the 4,941 retained hits. We reviewed the sample data against the list of permitted data elements above. We did not note any exceptions.

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. 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.

The ALPR system also records 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.

The Data Requests section of PBDTF's ALPR policy states:

> ALPR data that has been collected is classified as private unless access is permitted by law. Citizens can contact the system administrator to request ALPR data on their registered vehicles. This request is reviewed to ensure that it is consistent with the ALPR statute 13.824 and Minnesota Data Practices Act, Minnesota [Statutes], Chapter 13.

Commander Hart advised us that PBDTF has not had any requests for ALPR data from members of the public, but has received numerous requests from other law enforcement agencies. He advised us that ALPR data is shared only with agencies in Minnesota. PBDTF is able to provide direct access to those agencies that also use Flock Safety. In order to obtain access to PBDTF data, the requesting agency submits a signed ALPR Data Access Authorization form, which outlines the conditions of use, including the requirement that the requesting agency provide a case number and reason for each search, as well as the consequences of misusing ALPR data, which may include revocation of access as well as possible criminal penalties. Commander Hart reviews each application and, if approved, grants access to the requesting agency.

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.

The Paul Bunyan Drug Task Force uses only stationary ALPRs, and a complete list of the camera locations is available on the Minnesota Bureau of Criminal Apprehension website under the listing for the Beltrami County Sheriff's Office. With the exception of one camera that was experiencing power supply issues at the time of our audit, all of the deployed ALPRs are operational at all times. The Flock system captures the remaining elements from the list above and Commander Hart advised us that he generates a report containing this data once per month, with data aggregated for the preceding 30-day period. These reports are retained for a minimum of two years.

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, which is consistent with PBDTF's retention policy.

As part of the audit, Commander Hart furnished a link to PBDTF's "transparency portal," 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, and the law enforcement agencies with which PBDTF ALPR data is shared. While the transparency portal data does not satisfy all of the requirements specified for the public log of use, those remaining data elements are available in the reports Commander Hart creates each month.

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, Paul Bunyan Drug Task Force uses only stationary ALPRs. As part of this audit, Commander Hart furnished a list of stationary ALPR locations. Rampart compared this list to the list published on the Minnesota Bureau of Criminal Apprehension website under the Beltrami County Sheriff's Office and verified that both were identical.

We noted that while both state statute and PBDTF's BWC 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.

Commander Hart advised us that no PBDTF ALPRs have been moved since their initial placement; however, he retains copies of the emails used to notify the BCA of the initial placement, and will retain 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.

Commander Hart 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 limited to PBDTF agents, Beltrami County Sheriff's Office investigators, Bemidji Police Department detectives, the PBDTF administrative assistant, and one non-sworn criminal analyst each from PBDTF, BCSO and BPD. All users have search and alert access, but only PBDTF agents have hotlist update access. As part of the audit, Commander Hart furnished copies of signed memoranda from Beltrami County Sheriff Jason Riggs and Bemidji Police Chief Mike Mastin, documenting their written approval for BCSO investigators and BPD detectives, respectively, to be granted role-based access to PBDTF ALPR data, consistent with the requirement outlined in Minn. Stat. §13.824 Subd. 7(b).

Access is granted to a newly-assigned PBDTF agent only after he or she reads and signs off on the PBDTF ALPR policy, which spells out specific access rights based on job classification (position), the procedure that must be followed in sharing ALPR data with another law enforcement agency, the procedure that must be followed in releasing ALPR data to non-law enforcement persons or agencies, and the training and documentation requirements that pertain to ALPR data access. In addition, each new user completes individual ALPR system training with Commander Hart to ensure he or she understands the policy and procedures. Commander Hart also conducts monthly internal audits of ALPR system use to monitor for compliance.

As discussed in the Data Classification section of this report, PBDTF has a number of ALPR Data Access agreements in place with other Minnesota law enforcement agencies that use the Flock Safety system. Access to the Flock system itself is controlled by the external user's home agency, while access to PBDTF ALPR data is limited to the search function. All searches of PBDTF ALPR data by external personnel are logged and can be reviewed by Commander Hart. While the Data Access agreement requires that the external user provide both a case number and a reason for each search, Commander Hart lacks access to those agencies' records management systems (RMS) to verify that the search does in fact relate to the

provided case number. We noted, however, that this limitation would apply any time data sharing occurs between agencies.

Commander Hart advised us that the default configuration of the Flock system has been to make law enforcement agencies "discoverable" to other law enforcement agencies automatically, and to "opt-in" to data sharing by default. Commander Hart reviewed these settings with us during the audit, and we observed that the master data sharing option was deactivated. He confirmed that data sharing is only activated for individual agencies after he reviews and approves a signed PBDTF ALPR Data Access Authorization form.

As part of this audit, Commander Hart furnished a copy of the PBDTF ALPR Data Access Authorization form. We reviewed the sample form, noting that it addressed each of the elements contained in Minn. Stat. §13.824 Subd. 7(b) and (c).

Commander Hart advised us that the Flock system currently allows any authorized user to export ALPR data and does not document such activity in its audit trail. While the corresponding search for any data that was ultimately exported would still be logged, and the user would still be bound by both the ALPR data access agreement and state statute, it is our opinion that the process of downloading ALPR data likely constitutes "dissemination," for which a separate action that must be documented by the system. Commander Hart advised us that he has contacted Flock Safety about these concerns and generated a support ticket requesting that access to the export function be limited, and that all exports be recorded in the audit trail.

Because such data is not retained, Rampart was unable to complete our planned review of ALPR data exports as part of this audit.

AUDITOR'S NOTE RELATED TO DATA ACCESS

Minn. Stat. §13.824 Subd. 2(c) states in part: "A central state repository of automated license plate reader data is prohibited unless expressly authorized by law." Though the statute does not define the term "central state repository," we noted that when data sharing is active, the Flock system allows a user to conduct a single search for ALPR data retained by any or all of the agencies that have authorized data sharing with the requesting agency via the Flock system. Determining whether this functionality is compliant with the highlighted portion of Minn. Stat. §13.824 Subd. 2(c) above is beyond the scope of this audit.

ALPR DATA AUDIT TRAIL

Commander Hart ran an Audit Trail Report for the audit period. We noted that the audit trail documented searches conducted not only by PBDTF agents and BCSO and BPD personnel, but also by external agencies under approved ALPR Data Access agreements. Rampart reviewed a sample of the internal searches to verify that PBDTF's recordkeeping was accurate. One of the searches we reviewed

lacked a case or call for service number. Commander Hart immediately contacted the investigator who conducted the search and learned that it was related to a reported possible violation of a protection order.

Commander Hart also furnished a copy of a memo he created to document an internal ALPR audit he conducted on 10/08/2025 to illustrate the process he follows. The internal audit focused on agent use of custom hot-lists and traced the lone entry to a case number and a related tracking warrant. As part of his internal audit, Commander Hart verified both the case number and the existence of the warrant.

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 Paul Bunyan Drug Task Force's policy specifies a 60-day retention policy, Commander Hart advised us that the Flock Safety system limits data retention to 30 days. Settings in the flocksafety.com software automatically delete permanently any data contained in the ALPR database that is more than 30 days old. 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 an independent virtual server maintained by the Beltrami County Information Technology department.

As part of the audit, Commander Hart ran a report to list any retained ALPR data within the PBDTF ALPR database that was more than 30 days old. The report showed no retained data beyond the 30-day retention period.

INTERNAL CONTROL RECOMMENDATIONS

At the time of our audit, Commander Hart identified himself, the PBDTF administrative assistant and one criminal analyst each from the Beltrami County Sheriff's Office (BCSO) and the Bemidji Police Department (BPD) as the only users of the PBDTF ALPR system with Administrator access. Commander Hart advised us that Administrator rights were extended to the BCSO and BPD analysts in anticipation of sharing "hit" alert notifications directly with those agencies' patrol staff, as it would be more appropriate and practical for personnel from those agencies to set and monitor access rights for their own employees. Commander Hart advised us that this access can be revoked if this alert sharing does not occur.

We noted that, aside from the administrators, only agents assigned to PBDTF have access to update the Manual Hot List File, while all authorized users, including those from external agencies, have search and alert access to PBDTF ALPR data. In our opinion, this is to be expected given the PBDTF's use of the ALPR system as an investigatory tool, rather than one used primarily for traffic enforcement.

Commander Hart advised us that PBDTF agents and BCSO and BPD personnel are required to provide a reason for each search. He explained that while the use of a case or call for service number is also strongly recommended, the affected personnel normally have limited access to their RMS when operating in the field and may have an immediate need to search ALPR data without first verifying the correct case or call number. For that reason, the case/call number entry is not mandatory.

We recommend that a minimum of two administrators 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 Commander Hart to audit his own activity.

Commander Hart advised us that he is currently able to review 100% of internal search records. While describing his internal audit methodologies, we noted that he includes the following tests, which Rampart strongly recommends:

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 Paul Bunyan Drug Task Force'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 PBDTF's ALPR program is substantially compliant with the requirements of Minn. Stat. §13.824 and §626.8472, with the following exception:

- ALPR data downloads are not recorded in the data audit trail. In our opinion, such tracking is required under Minn. Stat. §13.824 Subd. 7(c). We note, however, that this is a limitation of the Flock Safety system, and that PBDTF is working with Flock to add this functionality.

Rampart Audit, LLC

11/28/2025

APPENDIX A:

Policy

613

Beltrami County

Sheriff's Office

Beltrami Cnty SO Policy Manual

AUTOMATED LICENSE PLATE RECOGNITION SYSTEM (ALPR)AUTOMATED LICENSE PLATE RECOGNITION SYSTEM (ALPR)

613.1 PURPOSE

Purpose: The purpose of this policy is to provide guidance on the access, storage and review of the Automated License Plate Recognition System (ALPR) and the use of data collected by the reader as well as the required system audits in accordance with Minn. Stat. 13.824.

613.2 POLICY

The Beltrami County Sheriff's Office (BCSO) recognizes the use of the ALPR as an effective tool to identify vehicles and vehicle owners who are associate with criminal activity and missing and endangered persons.

613.3 DEFINITIONS

Minnesota State Statute 13.824 defines an ALPR as an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on, or taking a photograph of, a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes. The law enforcement database is updated by the Minnesota Bureau of Criminal Apprehension (BCA) twice daily. Automated License Plate Reader includes a device that is owned or operated by a person who is not a government entity to the extent that data collected by the reader are shared with a law enforcement agency.

613.4 OPERATOR'S RESPONSIBILITY

(a) Use of LPR system shall adhere to the conduct policy (**1015; Conduct Policy**).

(b) Only officers trained in the proper use of the ALPR may operate it with their own unique login.

(c) When a "Hit" on the ALPR is received, the system will alert the user visually and audibly to the match. The user must acknowledge that the ALPR read the license plate correctly and verify the "Hit" is current by running the information through the state real-time data system via MDC or dispatch.

(d) Prior to taking enforcement action, the user or their designee shall verify that the vehicle description matches that given for the "Hit" vehicle. When a "Hit" is based on the status of the registered owner (i.e., license status, want or warrant) the user or their designee shall also verify when possible that the driver of the vehicle reasonably fits the physical descriptors given for the subject of the "Hit".

(e) Proper department procedures and safe police tactics should be followed when initiating a stop or investigation into a "Hit" vehicle.

(f) Any issues / problems with the ALPR system should be reported immediately to the system administrator.

(g) Any member who willfully violates Minn. Statute 13.09 through the unauthorized acquisition or use of ALPR data may face discipline up to and including suspension without pay or dismissal as a public employee.

613.5 DATA COLLECTED

Data collected by an ALPR must be limited to the following

(a) License plate numbers

(b) Date, time and location data on vehicles

(c) Pictures of license plates, vehicles and areas surrounding the vehicles

(d) Collection of any data not authorized above is prohibited

(e) Data collected by an automated license plate reader may only be matched with data in the Minnesota license plate data file, provided that a law enforcement agency may use additional sources of data for matching if the additional data relate to an active criminal investigation. A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law.

(f) Automated license plate readers 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 probably cause, or exigent circumstances justify the use without obtaining a warrant.

613.6 DATA STORAGE

(a) Data collected by an ALPR that are not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection. This allows a sufficient time frame for retrieving data relevant to a violation or criminal investigation.

(b) Preservation of data is required upon receipt of a written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and statement that the data may be used as exculpatory evidence. This data, otherwise subject to destruction after 60 days, must be preserved until the criminal charge or complaint is resolved or dismissed.

(c) Destruction of data is required upon written request from a program participant of "Data Protection for Victims of Violence." ALPR data related to the program participant must be destroyed at the time of collection or upon receipt of the request, whichever occurs later, unless the data is classified as active criminal investigative data.

(d) Data that are inactive criminal investigative data are subject to destruction according to the retention schedule for the data established under section 138.17.

613.7 AUTHORIZATION OF ACCESS

Access shall be permitted by the following:

(a) The ability of authorized individuals to enter, update or access ALPR 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, responses and all actions in which data is entered, updated, accessed, shared or disseminated must be recorded in a data audit trail or log.

(b) All request for ALPR data will be made to the system administrator or their designee.

(c) The data requested must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation and must include a record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.

613.8 SHARING OF INFORMATION

(a) Historical data records date, time, license plate number, GPS location, squad and camera information for each read. Historical data is only searchable for legitimate law enforcement purposes, outlined in ####.06 (above paragraph).

(b) Outside law enforcement requests for ALPR data should be routed to the system administrator or their designee.

(c) ALPR data is classified as private, with specific exceptions per Minn. Stat. 13.821.

(d) If data collected by an ALPR are shared with another law enforcement agency under this subdivision, the agency that received the data must comply with all data classification, destruction and security requirements.

(e) ALPR data that is not related to an active criminal investigation may not be shared with, disseminated to, sold to or traded with any other individual or entity unless explicitly authorized by state statute.

613.9 LOG OF USE

(a) Log of use is required to record specific times of day the reader actively collected data.

(b) Log of use is required to record 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 databases with which the data were compared, unless the existence of the database itself is not public.

(c) Log of use is required to record the number of vehicles or license plates where data identifies a vehicle or license plate that has been stolen, a warrant for the arrest of the owner of the vehicle or an owner with a suspended or revoked driver's license or similar category, or are active investigative data.

(d) Log of use is required to record an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

(e) A list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance device with ALPR capability, must be maintained. This list must be accessible to the public, unless it is determined that the data is security information.

613.10 HOT LISTS

(a) The ALPR is capable of alerting to license plates entered by the law enforcement agency in the ALPR system and not listed in the Minnesota License Plate Data File. Entries into the ALPR system shall comply with the following procedures and Minn. Stat. 13.824:

  (a) A license plate number or partial license plate number shall only be entered in a Manual Hot List when there is a legitimate and specific law enforcement reason related to an active criminal investigation to identify or locate that particular vehicle or any person reasonably associated with that vehicle.

  (b) Manual Hot List entries may only be made or edited by the system administrator or their designee.

  (c) A Manual Hot List entry shall be removed as soon as practicable if there is no longer a justification for the entry.

  (d) If an officer receives an alert based on a Manual Hot List entry, they must

follow ####.03 and confirm that current legal justification exists to act on the alert.

(e) A Manual Hot List entry may not be used as a substitute for an entry into any other databases such as Minnesota or FBI Hot Files, Nation Crime Information Center (NCIC), or Keeping Our Police Safe (KOPS) files, if appropriate.

613.11 BIENNIAL AUDIT

(a) It is required that records showing the date and time ALPR data was collected and the applicable classification of the data be maintained. An independent biennial audit of the records is required to determine whether data currently in the records is classified, how the data is used, whether they are destroyed as required and to verify compliance with the law.

(b) A report summarizing the results of each audit must be provided to the Commissioner of Administration, to the chair and ranking minority member of the committees of the House of Representatives and the Senate with jurisdiction over data practices and public safety issues and to the Legislative Commission on Data Practices and Personal Data Privacy, no later than 30 days following completion of the audit.

613.12 DATA REQUESTS

ALPR data that has been collected is classified as private unless access is permitted by law. Citizens can contact the system administrator to request ALPR data on their registered vehicles. This request is reviewed to ensure that it is consistent with the ALPR Statute 13.824 and Minnesota Data Practices Act, Minnesota Statues, Chapter 13.

613.13 NOTIFICATION TO THE BUREAU OF CRIMINAL APPREHENSION

ALPR data that has been collected is classified as private unless access is permitted by law. Citizens can contact the system administrator to request ALPR data on their registered vehicles.

This request is reviewed to ensure that it is consistent with the ALPR Statute 13.824 and Minnesota Data Practices Act, Minnesota Statues, Chapter 13.