2017

St. Paul Police Department
Automated License Plate Reader (ALPR)
Biennial Audit

Backbone Consultants
50 South Sixth Street, Suite 1360
Minneapolis, MN 55402
612 568-7167 |Tel
612 568-7187 |Fax

Backbone Consultants
50 South Sixth Street, Suite 1360
Minneapolis, MN 55402

Tel: 612-568-7167
Fax: 612-568-7187

info@backboneconsultants.com
www.backboneconsultants.com

December 21, 2017

Automated License Plate Readers (ALPR) Biennial Audit Results

The Saint Paul Police Department
367 Grove St.
Saint Paul, MN 55101

Backbone Consultants planned and performed an audit of the St. Paul Police Department's Automated License Plate Reader (ALPR) program to obtain reasonable assurance that it complies with the 2017 Minnesota Statute 13.824 AUTOMATED LICENSE PLATE READERS as of December 19, 2017.

Our testing included on-site testing of the ALPR application configuration settings, documentation reviews, and interviews with subject matter experts as it related to record classification, data usage, data destruction and authorization to access data.

Backbone Consultants determined that the St. Paul Police Department's Automated License Plate Reader (ALPR) program reasonably complies with the 2017 Minnesota Statute 13.824 AUTOMATED LICENSE PLATE READERS as it relates to the biennial audit requirements for record classification, data usage, data destruction and authorization to access data.

Because of its inherent limitations, projections of any evaluation of compliance to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate

Backbone Consultants

[redacted]

ALPR Biennial Testing Procedures

The following controls document the legislative requirements for St. Paul Police Department's Automated License Plate Reader program that are defined as in-scope per MN Statute 13.824 subd. 6 - Biennial Audit.

Control #	Process	Control Objective	Test Procedure	Test Results
1	Policy	A formal written ALPR policy has been created and approved by a chief law enforcement officer outlining the ALPR data classification, use, destruction, access controls, audit trail and breach notification.	Reviewed the current ALPR Operating Policy and validated the policy contains data classification, use, destruction, access controls, audit trail and breach notification.	No exception Noted
2	Data Classification	All data collected by an ALPR are private or nonpublic data unless the data are public under section 13.82, subd. 2, 3, or 6, or are active criminal investigative data under section 13.82, subd. 7	Reviewed the data classification defined in the ALPR Operating Policy and validated data is properly classified as nonpublic or private.	No exception Noted
3	Data Collection	Data captured by the license plate readers are limited to: (1) license plate numbers; (2) date, time, and location data on vehicles; and (3) pictures of license plates, vehicles, and areas surrounding the vehicles.	Reviewed the data fields collected by the ALPR application and validated fields were limited to license plate numbers, date/time/location data on vehicles, and pictures of license plates, vehicles, and areas surrounding the vehicles.	No exception Noted
4	Data Collection	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.	Reviewed data sources used to match against license plate reader data were all sources provided by the State of Minnesota.	No exception Noted
5	Data Collection	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 probable cause, or exigent circumstances justify the use without obtaining a warrant.	Reviewed the ALPR policy and validated tracking of individuals is explicitly prohibited. Reviewed data collected by the ALPR system and validated data is limited to approved vehicle metadata fields, data collected is from approved hotlists, and manual queries to search collected records requires the approved system user to enter a justification for the manual lookup.	No exception Noted
6	Data Retention	Data obtained from the license plate readers systems are destroyed within 60 days, unless part of a criminal investigation	Reviewed the ALPR system configuration and validated settings were properly configured to destroy data within 60 days of capture. Reviewed the data backups schedules for the servers hosting ALPR data and validated backups are not retained for greater than 60 days.	No exception Noted
7	Data Retention	Upon written request from an individual who is the subject of a pending criminal or complaint. Data otherwise subject to destruction must be preserved by the law enforcement agency along with the case or complaint number and a statement that data may be used as exculpatory	Reviewed processes to preserve data in the event of requests from subjects of a criminal investigation were made. At the time of the review, there had been no requests to preserve data by subjects of a criminal investigation.	No exception Noted

Control #	Process	Control Objective	Test Procedure	Test Results
		evidence until the criminal charge or complaint is resolved or dismissed.		
8	Data Retention	Upon written request from a program participant under chapter 5B, automated license plate reader 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 are active criminal investigative data.	Reviewed processes to destroy data in the event of requests from program participants were made. At the time of the review, there had been no requests to destroy data from a program participant.	No exception Noted
9	Data Classification	Request submitted under chapter 5B is classified as private data on individuals.	Reviewed the data classification defined in the ALPR Operating Policy and validated requests submitted under chapter 5B are classified as private.	No exception Noted
10	Data Retention	Data that are inactive criminal investigative data are subject to destruction according to the retention schedule for the data established under section 138.17	Validated policy and procedures are in place to destroy inactive criminal records in accordance to 138.17. Confirmed the ALPR system does not retain records past 60 days unless exported and exporting of records is managed by access controls and approved in writing.	No exception Noted
11	Access Control	Law enforcement agency must comply with section 13.05: The responsible authority shall: (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; (2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and (3) develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law. (b) When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.	Reviewed procedure documentation related to ALPR and ALPR data. Validated procedure documentation complies with legislation documentation requirements defined in section 13.05.	No exception Noted
12	Access Control	Law enforcement agency must comply with section 13.055. Disclosure of breach in security. Notification and Investigation report required.	Reviewed the data breach notification requirements defined within the ALPR Operating Policy	No exception Noted
13	Access Control	Written procedures to ensure that law enforcement personnel have access to the data only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency,	Reviewed the ALPR Operating Policy and access control procedures. Validated all current users with access to the ALPR system have a legitimate need for this	No exception Noted

Control #	Process	Control Objective	Test Procedure	Test Results
		or their designee, to obtain access to data collected by an automated license plate reader for a legitimate, specified, and documented law enforcement purpose.	access through documented approvals signed off by a designee of the Chief of Police.	
14	Access Control	Each access must be based on a reasonable suspicion that the data are 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.	Reviewed the ALPR system design and validated a mandatory dialog box to document a reason/justification for each manual query of the ALPR database is working effectively and cannot be bypassed. Validated the justification is retained in the system log.	No exception Noted
15	Access Control	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.	Reviewed the ALPR application uses role based access controls, all users were formally approval and were properly documented.	No exception Noted
16	Access Control	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	Reviewed the ALPR audit logs and validated the logs sufficiently capture all activity related to ALPR data, including, but not limited to, entering data, updating data, deleting data, searching data, changes to configuration settings, and changes to user accounts.	No exception Noted
17	Access Control	Formal approvals are captured and retained for every user with access to license plate reader data.	Reviewed all active ALPR user accounts and validated all users have a formal documented approval for access to the system and for a particular role.	No exception Noted

Additional Testing Procedures

The following controls were evaluated per the request of the St. Paul Police Department to assess their Automated License Plate Reader program to additional requirements defined in the MN Legislation which are outside of the biennial audit reporting requirements defined in MN Statute 13.824 subd. 6.

Control #	Process	Control Objective	Test Procedure	Test Results
18	Data Collection	Participation in a central state repository of ALPR data is prohibited only if the repository is explicitly authorized by law	Reviewed the ALPR configuration and validated St. Paul does not participate in a central repository for ALPR data.	No exception Noted
19	Sharing	Automated license plate reader data that are not related to an active criminal investigation may only be shared with, or disseminated to, another law enforcement agency upon meeting the standards for requesting access to data as provided in MN Statute 13.824 subdivision 7	Reviewed processes for sharing data which is not related to criminal investigations with external law enforcement agencies. Validated processes are in place to not share data without external law enforcement agencies meeting the standards for requesting access to data.	No exception Noted

Control #	Process	Control Objective	Test Procedure	Test Results
20	Sharing	External law enforcement agencies must follow Minnesota data classification, destruction, and security requirements when requesting data.	Reviewed processes to classify, destroy, and follow defined security requirements of data obtained from other agencies.	No exception Noted
21	Sharing	Automated license plate reader data that are 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 this subdivision or other law.	Reviewed processes to prevent for sharing of data not related to criminal investigations.	No exception Noted
22	Logging	A public audit log must be maintained, and include, but not limited to: (1) specific times of day that the reader actively 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 databases with which the data were compared, unless the existence of the database itself is not public; (3) for each period of active use, the number of vehicles or license plates in each of the following categories where the data identify 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; and (4) for a reader at a stationary or fixed location, the location at which the reader actively collected data and is installed and used.	Validate a public log is maintained. Validated all required data fields are captured per MN legislative requirements, including, time the readers were active per squad per day, aggregate number of vehicles scanned per day, number of positive hits in each required category. Reviewed all active devices configured within the ALPR system, validated fixed cameras were not in use.	No exception Noted
23	Logging	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.	Reviewed all active devices configured within the ALPR system, validated fixed cameras were not in use.	No exception Noted
24	Notification	The Bureau of Criminal Apprehension is notified of new fixed camera installations or changes to the locations of existing fixed cameras within 10 days	Reviewed all active devices configured within the ALPR system, validated fixed cameras were not in use.	No exception Noted
25	Notification	Within ten days of the installation or current use of an automated license plate reader or the integration of automated license plate reader	Reviewed the notice provided to the BCA by St. Paul PD indicating an active ALPR program.	No exception Noted

Control #	Process	Control Objective	Test Procedure	Test Results
		technology into another surveillance device, a law enforcement agency must notify the Bureau of Criminal Apprehension of that installation		