



Metropolitan Airports Commission

6040 - 28th Avenue South, Minneapolis, MN 55450 • 612-726-8100 • metroairports.org

January 24, 2018

Mr. Brian Ryks, Executive Director and Chief Executive Officer
Metropolitan Airports Commission

Mr. Roy Fuhrmann, Chief Operating Officer
Metropolitan Airports Commission

Mr. Mike Everson, Chief of Police, MSP Airport Police
Metropolitan Airports Commission

Gentlemen:

An audit of internal controls and compliance relative to MAC Automated License Plate Reader (ALPR) Technology has been completed and was conducted in accordance with the Standards for the Professional Practice of Internal Auditing. The following is a discussion of the objectives and scope of the work performed, background information and summary of results.

BACKGROUND

Automated License Plate Reader (ALPR) technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by MAC's Airport Police Department (APD) to convert data associated with vehicle license plates for official law enforcement purposes, which includes identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants and other authorized uses under Minnesota statute.

On August 1, 2015, Minnesota state legislation related to law enforcement's use of automated license plate readers went into effect. According to Minn. Stat. 13.824, Subd. 6, agencies using ALPRs shall arrange for an independent, biennial audit beginning August 1, 2017. The audit is to determine whether data currently in the agency's records are classified, how the data are used, whether they are destroyed as required in the statute, and to verify compliance with Minn. Stat. 13.824, Subdivision 7, which relates to authorization to access the data.

The statute mandates how the APD's data is collected, classified, and used. According to the statute, data collected must be limited to license plate numbers, date, time, location data on vehicles, and pictures of license plates, vehicles, and areas surrounding the vehicles. In addition, data collected by the readers are considered private data on individuals or nonpublic data unless the data are public under Minn. Stat. 13.82, Subd. 2, 3 or 6, or are active criminal investigative data under Minn. Stat. 13.82, Subd. 7. In addition, data collected may only be matched against data in the Minnesota license plate data file, but an enforcement agency may use additional sources of data for matching if the additional data relates to an active criminal investigation. ALPR

BACKGROUND (continued)

cannot 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.

Law enforcement agencies must also maintain a public log of its use, which would include information such as specific times of day the reader actively collected data, 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. Per Minn. Stat. 13.824 Subd. 5, the log should also include:

“(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.”

Besides determining how ALPR data is collected, classified, and used, the statute requires law enforcement agencies to destroy the ALPR data no later than 60 days from the date of collection. However, data may be kept longer than 60 days upon request of an individual who is subject of a pending criminal charge or complaint. In these situations, the data is kept until the criminal charge or complaint is resolved or dismissed. Unless there is a request by individual who is the subject of an ongoing investigation or complaint, MAC APD’s practice is more conservative than the requirement in the statute and destroys the data after 47 days (40 days + 7 days backup).

Regarding authorization to access data, the statute requires in Subd. 7(b):

“The responsible authority of a law enforcement agency establish written procedures to ensure 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, or their designee, to obtain access to data collected by an automated license plate reader for a legitimate, specified, and documented law enforcement purpose. Consistent with the requirements of paragraph (c), 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. (c) 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.”

The statute also requires law enforcement agencies to notify the Bureau of Criminal Apprehension (BCA) within 10 days of the installation or current use of an automated license plate reader or the integration of automated license plate reader technology into another surveillance device. The notification must also include any fixed location of a stationary automated license plate reader.

BOSS is the name of the APD’s system that tracks license plate data.

AUDIT OBJECTIVES

- To determine whether APD complied with the regulations stated in Minn. Stat. 13.824, which governs automated license plate readers.
- To determine whether APD's processes and procedures over ALPR are working as intended.

AUDIT SCOPE

The scope of our audit consisted of the compliance requirements stated in Minn. Stat. 13.824. Because the statute mandates ALPR data to be destroyed no later than 60 days from the date of collection, we reviewed ALPR data from the middle of May 2017 through July 2017.

AUDIT PROCEDURES

- Reviewed the Minnesota State statute that governs ALPR
- Obtained and reviewed MAC APD's policy regarding ALPR
- Interviewed MAC APD and IT staff to gain an understanding of the ALPR system (BOSS) and related processes and procedures
- Obtained a listing of users who have access to the BOSS system and their level of access
- Obtained a list of Minnesota license plate data files or "hot lists" within the BOSS system to which the ALPR data is compared against. These files contain information such as stolen vehicles, expired license plates, and missing children. MAC APD downloads this data from a Minnesota central repository on a daily basis.
- Obtained a listing of ALPR devices and locations within the BOSS system along with the setting for each device that shows when data is purged
- With the assistance of MAC IT staff, performed queries within the BOSS system to ensure data had been purged after 40 days as intended. (Data in the system is to be purged within 40 days whereas data that is located at off-site storage is purged after 7 days from when the off-site storage company received it.)
- Met with MAC IT staff to gain an understanding as to when ALPR data in offsite storage is purged and obtained examples from the offsite storage website showing the range of dates ALPR data was available
- Reviewed a sample of ALPR queries from the BOSS system audit log to determine the justification for the inquiries

AUDIT OBSERVATIONS

Observation #1 – User Access

During our review of a sample of inquiries made in the BOSS system, APD staff found that a user of the system had shared their logon credentials with another officer, who was not an authorized user of the system. This person was found to have used the ALPR system for legitimate law enforcement activities such as following up on license plate number matches against the Minnesota “hot list” data files. Minn. Stat. 13.824, Subd. 7 dictates how access to ALPR data is to be authorized and controlled. In addition, good business practices and related IT controls would suggest that access to systems should be limited and controlled by having separate log-on credentials for each user, and that authorized users should not share their log-on credentials with others who are not granted access to the system.

By sharing their log-on credentials with personnel who were not authorized to access the system, the police officers involved did not comply with the requirements in Minn. Stat.13.82, Subd. 7. In addition, errors or irregularities could take place and go undetected and potentially view private data.

Observation #2 – Use of Case Numbers

During our testing of a sample of ALPR system inquiries conducted by system users, we found that users of the system were not consistently inputting the case number or dispatch number in the system audit log to assist with proving justification for the ALPR inquiries. Case numbers for just 2 out of 14 system inquiries reviewed were properly entered in the ALPR system audit log. Ten of the remaining 12 were found to have been kept on a log outside of the system. According to Minn. Stat. 13.824, Subd. 7b, which addresses authorization to access data:

“Consistent with the requirements of paragraph (c), 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.”

Even though APD staff performed in-depth research to determine the justification for the ALPR inquiries in question, the process was rather time-consuming and justification for some inquiries were difficult to determine since they occurred several weeks prior from the date when the sample was pulled. By inputting case numbers or dispatch numbers into the ALPR system audit log, determining justification for ALPR system inquiries is made easier.

Observation #3 – Independent Review of System Audit Log

The ALPR system audit log is not independently reviewed on a routine basis. As required in Minn. Stat. 13.824, Subd. 7c, the ALPR system used by the APD does maintain an audit data trail (log), which records all actions performed in the system by users. However, we found that no one is reviewing the audit log on a routine basis. Reviewing system audit logs is an effective detective control that should be established with the implementation of most information systems. By not reviewing the audit log on a routine basis, errors or irregularities could occur and go undetected.

AUDIT OBSERVATIONS (continued)

Observation #4 – Authorization of User Access

The APD did not properly document its authorization of user access to the ALPR system. According to Minn. Stat. 13.824, Subd. 7b:

“The responsible authority of a law enforcement agency establish written procedures to ensure 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, or their designee, to obtain access to data collected by an automated license plate reader for a legitimate, specified, and documented law enforcement purpose. Consistent with the requirements of paragraph (c), 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. (c) 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.”

Our audit procedures found that the APD did not maintain written documentation as evidence that user access to the system was properly authorized. Without written documentation on file, we could not prove compliance with Minn. Stat 13.824, Subd. 7 and could not verify whether users of the system were properly authorized.

Observation #5 – Documentation of Training Users

The APD did not properly document whether users of the ALPR system were adequately trained prior to being granted access to the ALPR system. According to APD policy 462.4 (d), “No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.” Minn. Stat.13.824, Subd. 7c also refers to user access being limited “to the official duties or training level of the individual...”

We were informed that users did undergo in-depth training prior to being granted access to the system. However, records of the training were not kept on file. Without documented proper training, it cannot be demonstrated that users of the system understand the compliance requirements of the state statute and APD policy. In addition, errors or irregularities could occur. By not maintaining training records on file, we could not verify training compliance with either the APD policy or state statute.

Observation #6 – Data Classification

The APD policy does not contain language to address data classification as mentioned in Minn. Stat.13.824, Subd. 2b. which states, “All data collected by an automated license plate reader are private data on individuals or nonpublic data unless the data are public under Minn. Stat. 13.82, Subd. 2, 3, or 6, or are active criminal investigative data under Minn. Stat. 13.82, Subd. 7.”

AUDIT OBSERVATIONS (continued)

Although the APD does have language to address data collection and use restrictions, which are also requirements in statute, the policy does not address the data classification requirements.

Observation #7 – Maintenance of Public Log

The APD is not maintaining a public log of use as required per Minn. Stat. 13.824, Subd. 5. However, upon request, the APD has been able to pull the same information out of the ALPR system. Because the wording in the statute was ambiguous and the APD does have the ability to pull the data upon request, we contacted the Minnesota Department of Administration to obtain clarification. Their interpretation of the statute is that even though there is not a requirement to maintain an on-going public log, there is a requirement to maintain some form of log that is separate from the rest of the ALPR data and must contain the items listed in the statute.

AUDIT CONCLUSIONS

- In general, the APD complied with the regulations stated in Minn. Stat. 13.824, which governs automated license plate readers. However, the APD found an instance where a user of the ALPR system shared their log-on credentials with another officer who was not authorized to use the system. In addition, we did not find documentation on file proving that users of the ALPR system were properly authorized and were adequately trained. In addition, the APD policy should mirror the state statute and include language that addresses data classification. Plus, according to guidance obtained from the Minnesota Department of Administration, the APD should maintain a log that is separate from the ALPR system.
- In general, APD's processes and procedures over ALPR are working as intended. However, the APD should improve its process and procedures by implementing routine independent reviews of the ALPR system audit log. In addition, we found that users of system were not consistently documenting the case number or dispatch number in the system audit log as justification for ALPR system inquiries.

AUDIT RECOMMENDATIONS AND MANAGEMENT RESPONSE

MAC APD has reviewed this Automated License Plate Reader audit both internally and with MAC auditors. MAC APD has the following responses (*italics*) regarding the audit recommendations.

Recommendation #1 – User Access

Given the sensitive nature of ALPR data and compliance requirements in state legislation, MAC APD should take disciplinary action against the officer who shared their ALPR system credentials with another officer as well as against the officer who was given the credentials to perform inquiries in the system.

APD Response:

- *The MAC APD has disciplined the unauthorized user who accessed the system and the authorized user who provided their credentials. A copy of both discipline memorandums will be provided for documentation with audit. Individual's names were removed for privacy.*

Recommendation #2 – Use of Case Numbers

In order to assist in determining the justification for ALPR system inquiries and provide an audit trail, MAC APD should instruct all system users to input the case number or dispatch number in the system audit log.

APD Response:

- *All users of the system are now correctly entering their information into BOSS. These users will all be entering a case number or CAD event number. All system users have been re-trained.*

Recommendation #3 – Independent Review of System Audit Log

The MAC APD should improve its process and procedures over ALPR and conduct routine independent reviews of the ALPR system audit log. The reviewer should not be a user of the system.

APD Response:

- *A non-sworn civilian manager in the police department has been selected to work with MAC IT to perform a quarterly audit of the system. The MAC APD met with MAC Auditors, MAC IT and the MAC APD civilian manager to establish protocols to follow for the quarterly audits that will begin Q1 2018.*

AUDIT RECOMMENDATIONS AND MANAGEMENT RESPONSE (continued)

Recommendation #4 – Authorization of User Access

The MAC APD should improve its process over authorizing user access to the ALPR system and document the authorization in writing and keep the authorization documents on file.

APD Response:

- *The MAC APD civilian manager is responsible for authorizing user access to the ALPR system and maintaining written documentation of user records and training on file.*

Recommendation #5 – Documentation of Training Users

In order to determine whether users of the ALPR system have been adequately trained, the MAC APD should maintain written documentation of the training on file, which would include the user's signature and the date of the training.

APD Response:

- *The MAC APD has a documented training process which all of the users are trained in prior to being given access. MAC APD LPR trainer will notify the MAC APD civilian manager when a user successfully completes the ALPR standardized training at which point the manager can assign the individual a user name and password for the system.*

Recommendation #6 – Data Classification

The MAC APD should improve its policy governing ALPR and include language regarding the classification of the ALPR data as stated in Minn. Stat. 13.824.

APD Response:

- *The ALPR policy has been updated and is being sent out in to the department in Q4 2017.*

Recommendation #7 – Maintenance of Public Log

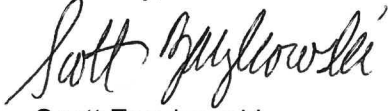
The MAC APD should maintain a public log of use that is separate from the ALPR system according to Minn. Stat. 13.824 Subd. 5 and guidance obtained from the Minnesota Department of Administration.

APD Response:

- *The MAC APD civilian manager will work with MAC IT in order to create and maintain a public log that is separate from the ALPR system that can be pulled on a routine basis.*

We would like to thank Chief Everson and APD staff for their cooperation and assistance in performing our audit procedures. We appreciate your responsiveness to our audit information requests. Please contact me at 612-467-0526, or Alan Sasse 612-725-6450 if you have any questions or concerns regarding this matter.

Sincerely,



Scott Zaczkowski,
Internal Audit Director



Alan Sasse, CPA/CISA
IT Audit Coordinator