

INDEPENDENT AUDIT REPORT

Director Carla Cincotta
MN Department of Public Safety
Alcohol and Gambling Enforcement
445 Minnesota St., Suite 1600
St. Paul, MN 55101

Dear Director Cincotta:

An independent audit of the Minnesota Department of Public Safety, Alcohol and Gambling Enforcement's (AGE) Portable Recording System (body-worn cameras (BWCs)) was conducted on May 14, 2024. The objective of the audit was to verify AGEs compliance with Minnesota Statutes §§13.825 and 626.8473.

Data elements the audit includes:

Minnesota Statute §13.825

- Data Classification
- Retention of Data
- Access by Data Subjects
- Inventory of Portable Recording System Technology
- Use of Agency-Issued Portable Recording Systems
- Authorization to Access Data
- Sharing Among Agencies

Minnesota Statute §626.8473

- Public Comment
- Body-worn Camera Policy

The AGE Division of the Minnesota Department of Public Safety employs nine (9) peace officers. AGE utilizes Axon body-worn cameras and Evidence.com cloud-based evidence management storage. The audit covers the period October 25, 2022, through April 30, 2024.

Audit Requirement: Data Classification

Determine if the data collected by BWCs are appropriately classified.

AGE's BWC data is presumptively private. All BWC data collected during the audit period is classified as private or nonpublic data. AGE had no incidents of the discharge of a firearm by a peace officer, use of force that resulted in substantial bodily harm, requests from data subjects for the data to be made accessible to the public, or court orders directing the agency to release the BWC data to the public.

No discrepancies noted.

Audit Requirement: Retention of Data

Determine if the data collected by BWCs are appropriately retained and destroyed in accordance with statutes.

AGE utilizes the MN Department of Public Safety AGE Division Records Retention Schedule and agency specified retention periods in Evidence.com. At the conclusion of a BWC recording, officers assign meta data, including an Evidence.com category, to the recording. Each Evidence.com category has an associated retention period. Upon reaching its retention date, evidence is systematically deleted. Deletion of the data is captured in the audit trail.

A report was produced from Evidence.com for all BWC data collected during the audit period. Records from the Evidence Created Report were reviewed, and the date and time the data was created was verified against the deletion date. Each of the records were deleted or maintained in accordance with the record retention schedule. Randomly selected audit trail reports were verified against the Evidence Created Report, and each record was deleted or maintained in accordance with the record retention.

AGE had received no requests from data subjects to retain BWC data beyond the applicable retention period.

Special Agents in Charge monitor BWC data for proper categorization to ensure BWC data are appropriately retained and destroyed.

No discrepancies noted.

Audit Requirement: Access by Data Subjects

Determine if individuals who are the subject of collected data have access to the data, and if the data subject requests a copy of the data, other individuals who do not consent to its release are redacted.

BWC data is available to data subjects and access may be requested by submission of a MN Department of Public Safety Data Request Form. During the audit period, AGE had received neither requests to view nor requests for copies of BWC video from data subjects.

No discrepancies noted.

Audit Requirement: Inventory of Portable Recording System Technology

Determine the total number of recording devices owned and maintained by the agency; a daily record of the total number of recording devices actually deployed and used by officers, the policies and procedures for use of portable recording systems by required by section 626.8473; and the total amount of recorded audio and video collected by the portable recording system and

maintained by the agency, the agency's retention schedule for the data, the agency's procedures for destruction of the data, and that the data are available to the public.

AGE's BWC inventory consists of nine (9) devices. An inventory report produced from Evidence.com detailed the total number of recording devices owned and maintained by the agency. The inventory included the device model, serial number, device name, the officer assigned to the device, date of last upload, device status, error status, firmware version, warranty date, date last docked, and camera state.

AGE's BWC policy governs the use of portable recording systems by peace officers while in the performance of their duties. The policy requires officers to ensure the BWC is functioning properly and to immediately notify their supervisor in the event of a damaged or malfunctioning device.

Peace officers were trained on the use of the portable recording system by Axon during implementation. Newly hired officers are trained as part of their field training program.

The BWC policy requires Officers working in the field during non-covert/non-undercover assignments to wear and activate BWCs. Officers working in the field on randomly selected dates were verified against the Evidence Created Report and confirmed that BWCs are being deployed and officers are wearing and activating their BWCs.

Evidence.com queries and the Evidence Created Report detail the total amount of BWC data created, stored/maintained, and deleted.

AGE utilizes the AGEs Records Retention Schedule and agency specified retention periods in Evidence.com. BWC video is fully deleted from Evidence.com upon reaching its scheduled deletion date. Meta data and audit trails are maintained in Evidence.com after deletion of BWC audio and video. BWC data is available upon request, and access may be requested by submission of a Department of Public Safety Data Request Form.

No discrepancies noted.

Audit Requirement: Use of Agency-Issued Portable Recording Systems

Determine if peace officers are only allowed to use portable recording systems issued and maintained by the officer's agency.

AGE's BWC policy states that officers may only use a BWC issued and maintained by the division and shall wear and operate it consistent with the policy and in the performance of official duties for the division or while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

No discrepancies noted.

Audit Requirement: Authorization to Access Data

Determine if the agency complies with sections 13.05, Subd. 5, and 13.055 in the operation of portable recording systems and in maintaining portable recording system data.

A special agent in charge reviews of BWC data to ensure BWCs are being used in compliance with policy.

Nonpublic BWC data is only available to persons whose work assignment reasonably requires access to the data. User access to BWC data is managed by the assignment of roles and permissions in Evidence.com. Permissions are based on staff work assignments. Roles and Permissions are administered by the Associate General Counsel and the Special Agents in Charge. Access to Evidence.com is password protected and requires dual authentication.

The agency's BWC Policy governs access to BWC data. Agency personnel may access BWC data for legitimate, specified law enforcement or data administration purposes and must be in the course and scope of the employee's job duties. User access to data is captured in the audit trail. The BWC policy states that employees failing to adhere to the policy or applicable laws regarding BWCs and its data, including but not limited to restrictions regarding accessing such data, may be subject to disciplinary action, up to and including termination, as well as criminal penalties pursuant to Minn. Stat. § 13.09 and Minn. Stat. §§ 13.825, subd. 12; 626.8473, subd. 3(b)(12).

When BWC data is deleted from Evidence.com, its contents cannot be determined. AGE has had no security breaches. A BCA CJIS Security audit was conducted in December of 2023.

No discrepancies noted.

Audit Requirement: Sharing Among Agencies

Determine if nonpublic BWC data is shared with other law enforcement agencies, government entities, or federal agencies.

AGE's BWC policy allows for the sharing of data with other law enforcement agencies prosecutors, courts and other criminal justice entities as provided by law. Law enforcement agencies seeking access to BWC data must submit a written request articulating a necessary, legitimate law enforcement purpose for the requested data. Sharing of data is documented in a police report and is captured in the audit trail. The Evidence.com Sharing Audit Report provides documentation of shared data.

No discrepancies noted.

Audit Requirement: Biennial Audit

Determine if the agency maintains records showing the date and time the portable recording system data were collected, the applicable classification of the data, how the data are used, and whether data are destroyed as required.

Evidence.com and the Evidence Created Report document the date and time portable recording system data were collected and deleted. All BWC data collected during the audit period is classified as private or nonpublic data. The Evidence.com audit trail documents how the data are used. The audit trail is maintained in Evidence.com after deletion of video. The Evidence.com audit trail documents each and every action taken from the creation of the recording to its deletion, as well as access to the audit trail after BWC has been deleted.

No discrepancies noted.

Audit Requirement: Portable Recording System Vendor

Determine if portable recording system data stored in the cloud, is stored in accordance with security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version.

An Axon CJIS Compliance White paper outlines the specific security policies and practices for Evidence.com and how they are compliant with the CJIS Security Policy. Axon has signed the CJIS Security Addendum in all states and has performed statewide CJIS-related vendor requirements in Minnesota. Axon has incorporated the CJIS Security Addendum by reference into the Axon Master Services and Purchase Agreement. Axon maintains signed CJIS Security Addendum certification pages for Axon personnel. Authorized Axon personnel are required to complete Level 4 CJIS Security Training upon assignment and biennially thereafter.

No discrepancies noted.

Audit Requirement: Public Comment

Determine if the law enforcement agency provided an opportunity for public comment before it purchased or implemented a portable recording system and if the governing body with jurisdiction over the budget of the law enforcement agency provided an opportunity for public comment at a regularly scheduled meeting.

AGE, as a state law enforcement agency, had no statutory requirement to provide an opportunity for public comment.

No discrepancies noted.

Audit Requirement: Body-worn Camera Policy

Determine if a written policy governing the use of portable recording systems has been established and is enforced.

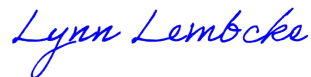
AGE has established and enforces a BWC policy. The policy was compared to the requirements of Minn. Stat. § 626.8473. The agency's policy includes all minimum requirements of Minn. Stat. § 626.8473, Subd. 3. The BWC policy is posted on the agency's website.

No discrepancies noted.

This report was prepared exclusively for the Minnesota Department of Public Safety, AGE Division by Lynn Lembcke Consulting. The findings in this report are impartial and based on information and documentation provided and examined.

Dated: July 30, 2024

Lynn Lembcke Consulting



Lynn Lembcke