Office of Internal Audit

# Performance Audit 20-04: Chattanooga Police Department Mobile Cameras

**February 2021**


**City Auditor**
Stan Sewell, CPA, CGFM, CFE

**Senior Auditor**
Jeff Connor, JD, CFE

# OFFICE OF INTERNAL AUDIT

**Stan Sewell, City Auditor**

February 25, 2021

To: Mayor Andy Berke
City Council Members

RE: Chattanooga Police Department Mobile Cameras Audit (Report #20-04)

Dear Mayor Berke and City Council Members:

The attached report contains the results of our audit of the Chattanooga Police Department (CPD) mobile cameras. Our findings confirmed that the CPD maintains sufficiently reliable and effective procedures governing the use and deployment of mobile cameras. However, our audit disclosed instances where procedures were not consistently followed, as well as opportunities to improve the retention model for mobile camera recordings.

To address the opportunities for improvement, we recommended the CPD implement additional safeguards and controls to ensure mobile camera recordings are downloaded, classified and reviewed in accordance with CPD policy. We also recommended the CPD adjust the schedule for retaining video recordings and data.

We would like to take this opportunity to thank the dedicated employees of the CPD for their courtesy, cooperation and assistance during this audit.

Sincerely,

Digitally signed by Stan Sewell
DN: cn=Stan Sewell, o=City of Chattanooga, ou=Office of Internal Audit, email=ssewell@chattanooga.gov, c=US
Date: 2021.02.25 14:45:25 -05'00'

Stan Sewell, CPA, CGFM, CFE
City Auditor

Attachment

cc: Audit Committee Members
Kerry Hayes, Chief of Staff
Maura Sullivan, Chief Operation Officer
David Roddy, Chief of Police
Eric Tucker, Deputy Police Chief
Glen Scruggs, Assistant Chief of Neighborhood Policing
Jim Arnette, Tennessee Local Government Audit

1001 Lindsay Street • Chattanooga, Tennessee 37402
(423) 643-6202 • FAX: (423) 643-6204 • E-MAIL: ssewell@chattanooga.gov

# TABLE OF CONTENTS

## AUDIT PURPOSE

This audit was conducted in accordance with the Office of Internal Audit's 2020 Audit Agenda. The objectives of our audit were to determine if: 1) policies and procedures governing the use of mobile cameras align with best practices for law enforcement agencies; and 2) police officers using mobile cameras are complying with established policies and procedures.

## BACKGROUND

The Chattanooga Police Department (CPD) uses mobile cameras (also referred to as "Digital Recording System" or "DRS" devices) to record interactions between police officers and the community they serve. When used properly, mobile camera devices promote transparency, foster accountability, and discourage inappropriate behaviors. However, without effective leadership and strong policy, merely outfitting police officers with cameras will not achieve desired results.

### How digital recording systems work

The CPD employs two (2) types of mobile camera devices: Axon-3 body-worn cameras and in-car recording devices.

*Body-worn Cameras (BWCs).* The Axon-3 is the latest generation of Taser-manufactured BWC mobile devices. Designed to capture activity within the officer's field of vision, the camera attaches to the chest area of the officer's uniform. The Axon-3 has two (2) operating modes. The buffering mode provides pre-event buffering to capture events prior to activating the event mode.[1] Once the event mode activates, it adds an additional 30 seconds of video to the beginning of the recording.[2] To deactivate the event mode, the officer simply presses and holds the event button, which returns the device to buffering mode.

*In-Car Video/Audio Recording System (ICVARS).* The ICVARS camera is a mobile recording device mounted inside the patrol vehicle. The camera can be positioned to record video inside and outside the vehicle. Once activated, the ICVARS camera continuously records until deactivated by the police officer.

---

[1] BWC devices are programmed to start recording automatically when the officer opens the door to the patrol vehicle, activates the vehicle's emergency lights, or draws his/her Taser weapon. A holster accessory is also available that can activate the camera when the officer draws his/her firearm.

[2] When the event mode is activated, the BWC device beeps twice to alert the officer the camera is recording.

## Capturing video

Police officers must activate their mobile camera device when they respond to calls for service or have citizen encounters where they anticipate taking law enforcement action. The device must remain activated from the beginning until end of the officer-citizen encounter.[3] In limited situations, police officers may discontinue a recording to develop rapport with a victim or maintain the confidentiality of a private citizen seeking to report information anonymously.[4]

## Downloading footage

At the end of a shift, when the officer returns the Axon-3 to its docking/charging station, the camera footage automatically downloads to a secure database that integrates with the Hamilton County 911 Computer Aided Dispatch (CAD) program. Downloaded recordings and CAD incident data are electronically linked by incident number.

## Classifying recordings

When emergency 911 calls are received, the CAD program systematically assigns an incident number and case type (*e.g.*, homicide, vehicle pursuit, felony investigation, *etc*.) used for video classification. Police officers are responsible for ensuring videos are appropriately classified as Non-Event, Limited, Intermediate, or Extended based on the events that occurred during the incident.[5] If the classification is questionable or unknown, officers must inform their supervisor and the supervisor is responsible for classification.

## Storing and retaining data

Recorded videos and associated data are stored on Evidence.com, a secure, cloud-based data system approved by the City's Department of Information Technology (DIT). The CPD retains downloaded recordings on the database in accordance with the following schedule:

- Non-Event: 0 days
- Limited: Minimum of 90 days
- Intermediate: Minimum of 24 months
- Extended: Indefinitely, but no less than 36 months

---

[3] In some instances, it may not be possible to capture images of an incident or an entire incident due to environmental conditions, the location of the officer, the location of the camera, or other factors.

[4] Police officers are encouraged (but not required) to record all interviews.

[5] Recoding classifications are individually described in the CPD Policy Manual.

## FINDINGS AND RECOMMENDATIONS

### Best practices for law enforcement mobile camera programs

The Commission on the Accreditation of Law Enforcement Agencies (CALEA) requires accredited agencies to maintain procedural controls over mobile camera programs. CALEA Standard 41.3.8 requires law enforcement agencies using mobile camera devices to implement written guidelines addressing: 1) situations for use; 2) data security and access; and 3) data storage and retention.

In addition, to develop uniform guidelines for law enforcement, the Police Executive Research Forum (PERF), in conjunction with the US Department of Justice Office of Community Oriented Policing Services (COPS), conducted a nationwide study on the use of mobile cameras.[6] The study consisted of three components: a survey of 500 law enforcement agencies nationwide, interviews with police executives, and a conference in which police chiefs and experts from across the country discussed best practices. Drawing on feedback from the conference, survey results, interviews, and policy reviews, PERF and COPS developed the following best practice recommendations for law enforcement mobile camera programs:

1) Develop specific criteria for device usage, including who will be assigned to use cameras and where the cameras are authorized to be placed;
2) Designate staff member(s) responsible for ensuring devices are charged and in proper working order, for reporting and documenting problems with devices, and for reissuing working devices to avert potential malfunction;
3) Implement clearly defined recording protocols, including when to activate the camera, when to turn it off, and the types of situations in which recording is required, allowed, or prohibited;
4) Adopt uniform processes for downloading recorded data, including who is responsible for downloading, when data must be downloaded, where data will be stored, and how to safeguard data against tampering or unauthorized deletion;
5) Establish procedures for documenting video evidence chain of custody;
6) Establish a video evidence retention schedule, specifying the length of time recorded data will be retained in various circumstances;

---

[6] Police Executive Research Forum, 2014, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*, accessed August 2020, <https://www.policeforum.org/assets/docs/FreeOnlineDocuments/Technology>

7) Establish a clear process for accessing and reviewing recorded data, including the persons authorized to access data and the circumstances in which recorded data can be reviewed;
8) Implement procedures for releasing recorded data to the public, including protocols regarding redactions and responding to public disclosure requests; and
9) Require that any contracts with third-party vendors for cloud storage explicitly state that the videos are police property, and use and access are governed by agency policy.

To determine if the CPD mobile camera policy aligns with best practices, we cross-referenced the CALEA requirements and PERF best practice recommendations to the corresponding provisions in the CPD Policy Manual. As illustrated in *Exhibit 1* below, CPD policy and procedures for mobile cameras comply with all CALEA requirements and best practice recommendations.

*Exhibit 1.*

| CALEA REQUIREMENTS | COMPLIANCE | CPD POLICY |
|---|---|---|
| *1) Situations for use* | *Yes* | *OPS-63 Section I.D-F* |
| *2) Data security and access* | *Yes* | *OPS-63 Section II.C-D* |
| *3) Data storage and retention* | *Yes* | *OPS-63 Section II.A-B* |
| **BEST PRACTICE RECOMMENDATONS** | | |
| *1) Camera use and location* | *Yes* | *OPS-63 Section I.C-E* |
| *2) Responsibility for ensuring cameras charged and functioning* | *Yes* | *OPS-63 Section I.C.3*<br>*OPS-63 Section I.G.1* |
| *3) Required and prohibited recordings* | *Yes* | *OPS-63 Section I.D-F* |
| *4) Process for downloading recorded data* | *Yes* | *OPS-63 Section I.H* |
| *5) Documenting chain of custody* | *Yes* | *OPS-63 Section I.E.4* |
| *6) Data retention schedule* | *Yes* | *OPS-63 Section II.B* |
| *7) Authorized access and review of recorded data* | *Yes* | *OPS-63 Section I.G*<br>*OPS-63 Section II.C* |
| *8) Public disclosure and redaction* | *Yes* | *OPS-63 Section II.D.8* |
| *9) Contract provisions for cloud storage* | *Yes* | *OPS-63 Section II.A* |

## Procedural enhancements for mobile camera use

Our audit confirmed that the CPD maintains sufficiently reliable and effective procedures governing the use and deployment of mobile cameras. In fact, our review of mobile camera recordings and data revealed no instances where police officers failed to record events required by policy, or improperly deactivated their cameras in violation of policy. To the contrary, in the videos reviewed, police officers maintained their cameras in record mode from the time they arrived at the scene of the incident until the conclusion of their involvement. However, our audit disclosed some instances where procedures were not consistently followed, as well as opportunities to improve the retention model for mobile camera recordings.

### Downloading delays

CPD policy requires police officers to download mobile camera recordings within two (2) hours of the end of their shift. In our review, we found recordings downloaded outside the timeframe prescribed by policy. Significant delays in downloading recordings limits access to recorded events that may be the subject of complaints or requests received immediately following the incidents.

**Recommendation 1**: We recommend the CPD implement additional safeguards and controls to ensure police officers download recordings in a timely fashion in accordance with policy.

***Auditee Response:*** *The current CPD policy on Body Worn Cameras requires officers to upload all data at the end of their shift barring exigent circumstances. The Department will develop and distribute a refresher training bulletin reinforcing this section of the policy and reminding supervisors to stay vigilant and address any lapses in adherence to policy.*

### Missing classifications and incident numbers

CPD policy requires police officers to classify recordings as Non-Event, Limited, Intermediate, or Extended. Saved recordings (except "Non-Event" recordings) must include the incident number, date, time, location of incident, identity of officer using the mobile camera, and any additional information useful to the incident. We found substantial numbers of saved recordings with no classification or incident number. The classification determines the length of time the recording is retained. Without a classification, the recording will be retained indefinitely. Without an incident number, the recording cannot be easily identified in a search, making it difficult for an interested party to locate recorded evidence related to a specific incident.

**Recommendation 2**: We recommend the CPD implement additional safeguards and controls to ensure saved recordings are properly

classified and assigned an incident number (unless classified as Non-Event) in accordance with policy.

***Auditee Response:*** *The current CPD policy on Body Worn Cameras requires an officer to properly classify all upload videos. The Department will develop and distribute a refresher training bulletin reinforcing this section of the policy and reminding supervisors to stay vigilant and address any lapses in adherence to policy. Additional safeguards on this item in Response 3.*

### Standardized review process

CPD policy requires supervisors to review at least two (2) recorded incidents for each mobile camera device issued every quarter. As part of the review process, supervisors are required to determine if the recordings were appropriately classified in accordance with policy. Our findings confirmed that supervisors performed the required number of reviews each quarter. However, the review documentation does not indicate whether the recordings were appropriately classified.

**Recommendation 3**: We recommend the CPD develop a uniform template for supervisors to use in evaluating mobile camera recordings. The template should indicate whether the recordings were created, downloaded, classified, and stored in accordance with policy.

***Auditee Response:*** *CPD will review and edit the existing template, if needed, and distribute to supervisors to use in documenting random reviews of officer's BWC videos. This review will include additional notations on the template of any unclassified or incorrectly classified videos and notations of any actions taken relative to the discovery of misclassified or no classification on BWC videos.*

### Retaining non-event recordings

CPD policy does not require the retention of Non-Event recordings. However, retaining Non-Event recordings for a reasonable time after an officer-citizen encounter enhances accountability for citizens and protects police officers from unfounded complaints.

**Recommendation 4**: We recommend the CPD extend the current retention schedule for Non-Event recordings from zero (0) days to seven (7) days.

***Auditee Response:*** *CPD will extend the retention period of Non-Event recordings from zero (0) days to seven (7) days by default on Axon software.*

# APPENDIX A: SCOPE, METHODOLOGY AND STANDARDS

Based on the work performed during the preliminary survey and our assessment of risk, the audit covers the use and deployment of CPD mobile cameras from January 1, 2020 to November 20, 2020. When appropriate, we expanded our scope to meet the audit objectives. We reviewed source documentation and data from Evidence.com, the Hamilton County CAD system, archived police reports, and daily activity logs. We used original records and copies as evidence verified through physical examination.

To develop our audit recommendations, we researched CALEA requirements and best practices for mobile camera programs. We reviewed CPD policy, procedural controls, and training materials. We interviewed CPD management, staff, and designated technical experts. We also conducted inspections of the mobile camera charging/downloading terminals and the CPD Real Time Intelligence Center (RTIC). Finally, we examined the security features, audit trial capabilities, and reporting tools of the Evidence.com database.

The sample size and selection of the data and recordings examined for the audit were statistically generated using a desired confidence level of 90 percent, expected error rate of five (5) percent, and a desired precision of five (5) percent. We used statistical sampling to extrapolate the conclusions of the test work performed on the data sample to the entire population from which it was drawn, and obtain estimates of sampling error. When appropriate, we used judgmental sampling to improve the efficiency of the audit.

We conducted this performance audit from August 2020 to January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our audit findings and conclusions.

**City of Chattanooga Fraud, Waste, and Abuse Hotline**

Internal Audit's Fraud, Waste, and Abuse Hotline gives employees and citizens an avenue to report misconduct, waste or misuse of resources in any City facility or department.

Internal Audit contracts with a hotline vendor, Navex Global, to provide and maintain the reporting system. The third party system allows for anonymous reports. All reports are taken seriously and responded to in a timely manner. Reports to the hotline serve the public interest and assist the Office of Internal Audit in meeting high standards of public accountability.

To make a report, call 1-877-338-4452 or visit our website:
*www.chattanooga.gov/internal-audit*