Auditing Body-Worn Camera Programs

Rebecca S. Robinson and Ivy Williams
*Performance Auditors, City of Atlanta*
Overview

- Short Program History
- Audit Objectives
- Criteria & Methodology
- Audit Findings
- Testing Possibilities
Short Program History

- Body-worn cameras promote transparency and accountability and discourage inappropriate behavior

- National media attention begins to highlight police killings of unarmed black men, such as:
  - Eric Garner (July 2014)
  - Michael Brown, Jr. (August 2014)

- In 2015, Obama secures Department of Justice funding for BWC pilot programs
APD Explores BWC Options

- In 2015, Atlanta Police Foundation conducted a pilot study to determine departmental needs
- In 2016, city council passed a resolution to procure 1,200 Axon Body 2 devices from Taser International
- APD began rolling out BWCs in November 2016, starting with Zone 4
Audit Objectives

- Do body-worn camera users comply with the Atlanta Police Department’s standard operating procedures?
- What metrics should the Atlanta Police Department consider when assessing officers’ compliance with policy and best practices?
Criteria

- Best Practices
  - Police Executive Research Forum (PERF)
  - NYPD Inspector General’s Office
  - Bureau of Justice Administration (BJA)

- APD Body-Worn Camera Policy
  - Officers’ Responsibility
  - Supervisors’ Responsibility
  - Compliance Administrator’s Responsibility
Policies & Procedures

- Trained staff ranked at sergeant and below must use BWCs

- Revisions in January and December 2017
  - Retention schedule changed to 5 years for all violations except homicide in June 2018
  - Officers must activate BWCs for all service calls

<table>
<thead>
<tr>
<th>Violation</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Stop</td>
<td>180 Days</td>
</tr>
<tr>
<td>Citation</td>
<td>180 Days</td>
</tr>
<tr>
<td>Citizen Contact</td>
<td>180 Days</td>
</tr>
<tr>
<td>Criminal Investigation</td>
<td>30 Months</td>
</tr>
<tr>
<td>Use of force w/no arrest</td>
<td>30 Months</td>
</tr>
<tr>
<td>Arrest</td>
<td>5 Years</td>
</tr>
<tr>
<td>Homicide</td>
<td>Indefinite</td>
</tr>
</tbody>
</table>
Officers’ Responsibilities

- Officers’ responsibilities:
  - Ensure proper function
  - De/activate (upon arriving on scene/when the event has transitioned to a controlled situation)
  - Charge/upload
  - Categorize videos after uploading footage
  - Report interruptions/failures to activate
Supervisors’ Responsibilities

- Zone supervisors:
  - Inspect equipment at the start-of-shift
  - Ensure officers follow policy
  - Record officer or citizen-initiated calls
  - Prevent misuse of equipment
  - Upload UOF videos
Compliance Administrator

- Compliance administrator:
  - Audit footage: semi-annually; changed to random audit of 25 videos weekly
  - Submit violations of local, state, and federal standards to OPS
  - Maintain a list of users
  - Manage Evidence.com
  - Respond to open records requests (redaction)
Device Specifications

- Lens
- Speaker
- EVENT Button
- Microphone
- On/Off Switch
- Function Button
- Battery LED
- Battery Status Button
Device Specifications
Specifications (cont’)

- Multicam: automatically links videos based on geolocation and time
Methodology

- Tests through Evidence.com data:
  - Difference between video creation and upload
  - Officer upload at end-of-shift
  - Uncategorized footage
  - Supervisors upload UOF/time to upload
  - Supervisory review
  - Video deletion
  - Compliance audits

- CAD and Evidence.com data:
  - Calls without videos
Methodology

- Conducted tests through video observation:
  - De/Activation
  - Miscategorization

- Reviewed police incident reports and Evidence.com data:
  - Officers review UOF

- Ride-alongs
  - Supervisors upload UOF
  - Uncategorized
  - Supervisory review
Methodology

- We relied on the below reports from Evidence.com:
  - Evidence Created
  - Evidence Deleted
  - User Audit Trails

- CAD data from June 2017 to May 2018

- Incident reports

- Ride-alongs in the 6 police zones
Developing a Testing Plan

- Craft a plan that answers the audit objectives
- Identify data fields and understand what they mean
- Conduct short pilot tests to deter “scope creep”
- Consult the auditee during testing
Test 1

- We conducted a representative statistical sample based on
  the number of videos created in each zone (150 total)

- We observed videos for the following elements: category
  (proper), case number, buffer, code 2/3 driving, activation
  upon arriving on scene, deactivation upon conclusion of
  event, number of videos associated with case number, and
  available MC footage

- **SOP:** Officers must activate before arriving on scene or while
  driving code 2 or 3 (in practice, some activate after radioing
  in, others as they exit their vehicles); officers must deactivate
  when the event has ended or transitioned to a controlled
  situation (some when they radio in)
Test 1 Findings

- **Activation:** 52-68%
- **Deactivation:** 39-55%
- **Both:** 30-46%

150 Total Sampled
Test 1 Findings (cont’)

- Multiple videos: 22%
- Multicam: 60%
- No buffer: 16%
- Miscategorized: 15% (including 1 UOF)
Test 1

- **Compliance team audit**: category added, activation before arriving on scene, buffer, obstructed view, audio and video of acceptable quality, associated incident report, and BWC box checked in ICIS.
Test 2: Officer upload

- Used the “days_between_create_and_upload_date” field on the Evidence Created report

- **SOP:** Officers should dock their BWCs, initiating the upload, at the end of their shift (in practice, some officers leave immediately for their second jobs, which also require the use of the BWCs, after their regular shifts end; BWC team said a 3-day window for uploading is more reasonable)
Test 2 Findings

- Officers uploaded 74% of videos within a day, 88% within 3 days, and 95% with 9 days.
Test 3: Uncategorized video

- We compared the Evidence Created (total videos) to the “Uncategorized Evidence” report

- **SOP:** Officers must add categories and case numbers to videos at the end of their shifts
Test 3 Findings

- Less than 0.4% (1,780) of 491,753 videos were uncategorized; failed to add case numbers to 10%.

- Officers failed to categorize 2/3 of the uncategorized videos in the months during and just after the malware attack (March-May 2018).
Test 4: CAD calls with video

- We compared the CAD report (after removing non-LE entries) to available videos.
- E911 dispatchers assign calls (with case numbers) to officers and dispatchers generate case numbers for self-initiated calls.
- **SOP:** Officers should record all service calls (about 80% in practice).
Test 4 Findings

- 67% of CAD calls had no corresponding BWC footage
Test 5: Supervisors upload UOF

- We filtered videos categorized as UOF and compared “owner_badge_id” and “uploaded_by_badgeid” fields

- **SOP:** After a UOF event, supervisors should upload/categorize the footage before the end of the shift; officers may not review it until after making a statement
Test 5 Findings

- Less than 1% of videos were categorized as UOF (1,480) and 27% of them were uploaded by a supervisor.

- A supervisor in the field told us that he does not upload UOF videos.
Test 6: User justifications

- We filtered the videos that users had streamed and used the “notes” field to see if they had posted notes justifying their reasons for streaming the footage

- **SOP:** All users are required to leave justifications in the “notes” field to uphold the chain of custody
Test 6 Findings

- 20% of streamed videos had justification notes
- No standardization; some notes were not justifications (i.e., case numbers or locations)
Test 7: Supervisory review

• We downloaded supervisors’ audit trails and calculated how many times they streamed officers’ videos

• **SOP:** Silent on requirements, except “ensure compliance,” but best practices suggest that supervisors should randomly audit videos to ensure compliance and performance standards
Test 7 Findings

- Supervisors streamed 2% of videos
- Only 1 out of 148 supervisors streamed officers’ videos on a monthly basis
- Some supervisors told us they did not have a process for reviewing videos
- Best practices: monthly sample of randomly selected videos
Test 8: Supervisors upload times

- We filtered UOF videos and used the “days_between_create_and_upload_date” field on the Evidence Created report.
- **SOP**: Supervisors must upload UOF footage by the end of the shift.
Test 8 Findings

- Average: 3 days
- Median: 0 days
- Not included in report
Test 9: Officer review of UOF

- We compared sampled 48 UOF incident reports to Evidence Created data
- **SOP**: Officers must make statements before reviewing UOF videos
- Officers completed statements after supervisors uploaded videos 60% of the time
- Test canceled because timestamp on the incident reports was inaccurate
Test 10: Supervisor inspections

- We initially planned to extract device audit trails to ascertain whether devices were powered on and fully charged at the beginning of officers’ shift but we decided that it would be too difficult to determine officers’ scheduled

- Test canceled

- Testing possibilities
Test 11: Deletion by category

- We determined the length of retention based on the Evidence Created report’s “evidence created” and “date deleted” fields and compared it with the “category” field.

- **SOP:** Not covered in written policy; BWC team told us that 2 members are able to delete videos.
Test 12: Deletion by role

- Based on the findings from Test 11, we used the "deleted_by_role" from the Evidence Created report to determine whether a superadmin had deleted videos.
Test 11 and 12 Findings

- Evidence.com deleted 99% of videos according to their retention schedule
- 86 were manually deleted (63 categorized): 26 by administrators, 37 by supervisors, 23 uncategorized and deleted by supervisors
Test 13: Lost/damaged BWCs

- We requested documents from the compliance team but they were lost in the malware attack
- We canceled this test
Test 14: Compliance team audits

- We extracted the user audit trails for the compliance team to determine if members randomly audited 25 pieces of evidence per week.

- **SOP (revised):** Compliance administrator must audit 25 pieces of data per week.
Test 14 Findings

- Compliance team reviewed 1,325 videos (>1%)
- The team audited the required number of videos in 3 out of the 6 months after the department revised the policy
Test 15: Administrator review of videos queued for deletion

- We examined the audit trail of the administrator who was responsible for reviewing videos that are queued for deletion.

- **SOP:** Not into written policy
Test 15 Findings

- The administrator reviewed less than 1% of videos before their deletion.
- We recommended ranking videos queued for deletion based on risk (e.g., training and accidental videos that are longer than 2 minutes).
Testing Possibilities

- Checking for video/audio quality
- Checking dock to see if BWCs are having data transfer issues and if they are being addressed (i.e., function LED blinking green/yellow (transfer error) or red/yellow/green (network error))
- Examining video shares (with whom and for what purpose)—may require examining audit trails
- Roll call for supervisory inspection (charged and powered on)
- Miscategorization through incongruence of multiple categories
Testing Possibilities

- Sample of high-risk videos in terms of categorization
- Check if all cameras are assigned to a person
- Check lost/damaged BWCs and forensic assessment (if damaged)
- Investigate performance metrics: reductions of complaints (all and those that were sustained)
- Perform cost-benefit analysis: how much would city pay in lawsuits without evidence to clear officers of wrongdoing? How often is footage used by courts and OPS?
Testing Possibilities

- Check if supervisors are recording citizen initiated requests (observed a shots fired event in which supervisor’s BWC was not even powered on)
- Obstructed views
- Proper documentation (incident reports reference video)
Thank you!

Questions?