LAW ENFORCEMENT BODY CAMERA TASK FORCE

Recommended Regulations for the Procurement and Use of Body Worn Cameras by Law Enforcement, August 2, 2022

I. INTRODUCTION

A. Background

The legislature created the Law Enforcement Body Camera Task Force in the Act Relative to Justice, Equity, and Accountability in Law Enforcement in the Commonwealth, otherwise known as the police reform law, for the purpose of drafting recommended regulations for the procurement and use of body-worn cameras by law enforcement officers, and minimum requirements for the storage and transfer of audio and video recordings collected by body-worn cameras. St. 2020, c. 253, § 104.

As required by the statute, the Executive Office of Public Safety and Security (EOPSS), in collaboration with the Executive Office of Technology Services and Security (EOTSS), established the Law Enforcement Body Camera Task Force (Task Force). The Task Force has completed its work and recommends the procurement policy and body worn camera policy contained herein, which are consistent with the statutory requirements.

Section 104 of Chapter 253 of the Acts and Resolves of 2020 required the Task Force to establish the following:

- Standards for the procurement of body-worn cameras, including a requirement that such cameras or associated processing software include technology for redacting the images and voices of victims and by-standers;
- Standards regarding the use of facial recognition or other biometric-matching software or other technology to analyze recordings obtained through the use of such cameras; provided, however, that such standards may prohibit or allow such use subject to requirements based on best practices and protocols;
- Standards for training law enforcement officers in the basic use of such cameras;
- Standards for:

  (A) The types of law enforcement encounters and interactions that shall be recorded and what notice, if any, shall be given to those being recorded; and

  (B) When a camera should be activated and when to discontinue recording;
- A requirement that a camera be equipped with pre-event recording, capable of recording at least the 30 seconds prior to camera activation;

- A requirement preventing an officer from accessing or viewing any recording of an incident involving the officer before the officer is required to make a statement about the incident;
- Standards for the identification, retention, storage, maintenance, and handling of recordings from body cameras, including a requirement that recordings be retained for not less than 180 days but not more than 30 months for a recording not relating to a court proceeding or ongoing criminal investigation or for the same period of time that evidence is retained in the normal course of the court's business for a recording related to a court proceeding;
- Standards pertaining to the recordings of use of force, detention or arrest by a law enforcement officer or pertaining to ongoing investigations and prosecutions to assure that recordings are retained for a period sufficient to meet the needs of all parties with an interest in the recordings;
- Standards for the security of facilities in which recordings are kept;
- Requirements for state procurement of contracts for body-worn cameras and for data storage through which qualified law enforcement agencies may purchase goods and services;
- Best practice language for contracts with third-party vendors for data storage, which shall provide that recordings from such cameras are the property of the law enforcement agency, are not owned by the vendor and cannot be used by the vendor for any purpose inconsistent with the policies and procedures of the law enforcement agency;
- Procedures for supervisory internal review and audit;
- Sanctions for improper use of cameras, including a requirement that a law enforcement officer who does not activate a body-worn camera in response to a call for assistance shall include that fact in their incident report and note in the case file or record the reason for not activating the camera;
- Sanctions for tampering with a camera or recordings and for improper destruction of recordings;
- Regulations pertaining to handling requests for the release of information recorded by a body-worn camera to the public;
- Requirements for reporting by law enforcement agencies utilizing body-worn cameras;
- Retention schedule for recordings to ensure that storage policies and practices are in compliance with all relevant laws and adequately preserve evidentiary chains of custody and identify potential discovery issues; and
- Process by which body camera footage may be included in a public record.

B. Task Force Supplemental Recommendations

The Task Force discussed three additional issues at length and concluded that the importance of these issues warrant inclusion in this report, although they do not fall directly within the scope of the statute's requirements.

1. It is the belief of the Task Force that the financial impact of a body worn camera program on respective police departments is significant. While implementation of a program serves communities, it requires significant financial support to launch and maintain a program. It is the consensus of the Task Force that individual police departments seek adequate financial support from all available funding sources, including cities, towns, as well as the Commonwealth's leadership, to budget for a body worn camera program accordingly. Proposed financial cost projections should be provided to the respective leadership in the town/city, to the extent that it can be.

2. It is the Task Force's opinion that the video retention policy they are required by the statute to recommend, which is 30 months, be extended to 37 months because a 30-month retention policy may adversely impact parties in a civil action filed after the expiration of the 30 months but before the statute of limitations runs for civil cases, which is 3 years. In addition, the "not less than 180 days" statutory retention requirement does not allow sufficient time to determine whether recordings need to be accessed. Therefore, although the Task Force is required to recommend "not less than 180 days," consideration should be given to retaining the footage for one year.

3. The Task Force heard from the public on the issue of an officer's access to the BWC video footage, and more specifically on the issue of when such access should be given for the purpose of making a written statement concerning an event. While the Task Force discussed the issue, and the members had differing views on what the recommended regulation should be, the legislature constrained the Task Force's ability to offer a recommendation other than that imposed by the statute, which requires that the Task Force make the following recommendation:

- An officer may not access or view "any recording of an incident involving the officer before the officer is required to make a statement about the incident;"

Accordingly, this is the recommendation in section R.5.2, which concerns on-duty requirements.

Sincerely,

The Law Enforcement Body Camera Task Force

LAW ENFORCEMENT BODY CAMERA TASK FORCE MEMBERS

Angela F.F. Davis, Assistant Undersecretary of Law Enforcement and Criminal Justice
Chair, Secretary of the Executive Office of Public Safety and Security Designee

Major Steven McCarthy
Vice-Chair, Colonel of the Massachusetts State Police Designee

Timothy Mitchell, Operations Project Management, Office Director
Secretary of the Executive Office of Technology Services and Security Designee

Stephen J. Carley, Esq.
Assistant Attorney General Attorney General Designee

Rose King, Esq.
Committee for Public Counsel Services Designee

Grace Lee, Esq., People's United Bank
Massachusetts House Asian Caucus Designee

Steven Brooks, Esq., Brooks & Crowley, LLP
Massachusetts House Asian Caucus Designee

Officer Israul Marrero, Boston Police Department
Massachusetts Minority Law Enforcement Officers Association Designee

Lieutenant (Ret.) Carmelo Ayuso, Massachusetts State Police
President, Massachusetts Minority State Police Officers Association Designee

Officer Kaleigh S. Marshall, Chelmsford Police Department
Massachusetts Association of Women in Law Enforcement Designee

Patrick McDermott, Norfolk County Sheriff
President, Massachusetts Sheriffs' Association Designee

Sergeant Timothy King, Waltham Police Department
Massachusetts Coalition of Police Designee

Michael O'Keefe, Cape and Islands District Attorney
President, Massachusetts District Attorneys Association Designee

Emiliano Falcon-Morano, Esq., Policy Counsel
President, American Civil Liberties Union of Massachusetts Designee

Fred Taylor
President, NAACP New England Area Conference Designee

Alyssa Hackett, Esq.
President, Massachusetts Criminal Defense Lawyers Association Designee

Chief Steven M. Sargent, Worcester Police Department
Gubernatorial appointment: Police Chief, City with population in excess of 100,000

Chief Thomas W. Fowler, Salisbury Police Department
Gubernatorial appointment: Police Chief, City or Municipality with population no greater than 50,000

Hillary Farber, Esq.; Professor of Law, University of Massachusetts School of Law
Gubernatorial appointment: Constitutional or Privacy law expert

Mayor Dominic Sarno; City of Springfield
Gubernatorial appointment: Elected Official

Deborah Batista, Executive Vice President; New England Police Benevolent Association, Inc.
Gubernatorial appointment: Representative of a law enforcement labor organization

*Please be advised, the Chief Justice of the Supreme Judicial Court declined to make an appointment, and the Massachusetts Black and Latino Legislative Caucus did not make two appointments.

Executive Office of Public Safety and Security Staff:
Suleyken Walker, Esq.; EOPSS Deputy General Counsel, Task Force Counsel
Dan Nakamoto; EOPSS Chief Operating Officer, Task Force Advisor
Michaela Martini; EOPSS Criminal Justice Advisor, Task Force Staff
Amy Putvinskas; EOPSS Program Coordinator, Task Force Staff

The Task Force devoted an extensive period of time discussing various viewpoints to ensure that all stakeholder groups, individuals, and members of the public were considered in the creation of these recommended guidelines.

STATEMENT OF PURPOSE OF BODY CAMERAS

The purpose of body worn cameras is to:

- Improve community relations;
- Foster better accountability for the actions of its personnel;
- Deter or document inappropriate conduct by police officers and by members of the public;
- Capture digital audio-video evidence for criminal, civil, and traffic-related court cases;
- Assist with training officers; and
- Improve the quality of interactions between officers and the members of the public.

DEFINITIONS

Activation: The action of initialization or making a unit active.

Audit log: A system or document that records what sources were accessed, when, by whom.

Body Worn Camera (BWC): Wearable integrated audio/video recording equipment.

Body Worn Camera User (BWC User): An individual as prescribed by a law enforcement or public safety agency charged with the use of a Body Worn Camera in accordance with recommended regulations. All law enforcement officers who would reasonably be expected to interact with members of the public shall wear a body camera, in accordance with department policy.

Digital Evidence: Data or information which is stored that may be used as evidence in legal proceedings.

Equipment Standards: Defined metrics for conformity and usage of equipment to meet a threshold of performance expectations.

Labeling/categorizing/tagging video: The process of labeling content of a video, identifying specific information for future reference.

Light Emitting Diode (LED): A semiconductor diode which glows when connected to voltage.

Metadata: Data which describes or provides contextual information about content or other data such as a text or image.

Post Event Recording: The ability of the BWC to create a recorded event from the device memory even if the user did not activate the recording feature of the BWC. Post Event Recording capabilities vary by manufacturer.

Pre-event recording: The ability of a BWC to capture video from its memory buffer.

Wide High Dynamic Range Camera: Technology enhancing capability of capturing images, light and view.

RECOMMENDED REGULATION FOR THE PROCUREMENT OF BODY CAMERAS

R.1 EQUIPMENT STANDARDS

R.1.1 - Tamper Resistant

BWCs proposed by the vendor should prevent recordings from being edited or deleted, nor should it be possible to overwrite the existing data before it has been transferred from the recording device and stored. The vendor should describe, in detail, how video and audio recordings are protected.

R.1.2 - Device Storage

BWCs should have a minimum of 16 hours of high-definition video recording time with non-volatile, onboard storage. BWC storage may be less, provided that captured video is offloaded during, or immediately after, recording. Storage for offloaded data should meet the tamper resistance requirements. The vendor should specify the maximum onboard memory storage capacity of its BWC unit.

R.1.3 - Battery

BWCs should have a battery which provides a minimum of 8 hours of recording time (with a hot swappable battery solution) or a minimum of 12 hours of recording time (with a battery integrated into the BWC). Batteries should be rechargeable. Camera equipment should include a visible charging indicator to show active charging and full charged status. The vendor should specify (1) if its battery is internal or removable, (2) the recording life of the camera battery, (3) the standby duration of the battery, (4) battery charging time, and (5) whether the camera can be charged without docking and uploading the video (the vendor should describe how this is accomplished with its product).

R.1.4 - Durability

BWCs should withstand considerable and repetitive pressure, vibration, and mechanical shock. It should operate within a temperature range from -20F to 125F and be resistant to common environmental hazards, such as dust, condensation, water splashes, and radio frequency interference. Equipment should meet the MIL-STD-810G or similar standard. The vendor should describe the tests used on its devices (e.g., drop test, operating temperatures, vibration, water resistance, etc.) in its documentation. The BWC unit should be a ruggedized, military/industrial grade device capable of functioning normally in harsh environments and in adverse weather conditions. The vendor should describe in its documentation whether its product is intrinsically safe in a potentially explosive environment.

R.1.5 - Weight and Form Factor

The BWC proposed by the vendor should not distract or hinder the BWC user wearing the device from performing other job functions, especially ones related to user safety. BWCs should be designed for maximum usability and safety. The vendor should specify the physical dimensions of the BWC (including the camera, control unit, and battery), along with the weight of the BWC unit.

R.1.6 - Camera Mounting

The BWC should be capable of attaching to the user's uniform using secure mounting options, while providing full unobstructed recording. The vendor should fully specify varied mounting options provided.

R.1.7 - Device Management

Vendors' proposed systems should have the capability of pushing configuration and software upgrades wirelessly to connected cameras without necessity of any user input. The agency should set requirements for periodic upgrades of equipment that do not interfere with its operation.

R.1.8 - Digital Channels

The wireless recording devices should utilize individual channels to avoid multiple devices interfering with each other. The vendor should specify the maximum number of channels supported by its solution.

R.1.9 - Auto Stop

The system should have a means of detecting when the system is inadvertently left in record mode. The system should allow an option to prompt the user or to automatically stop the recording.

R.1.10 - Disk Usage Meter and Low Disk Warning

If the vendor-proposed solution includes the storing of video recordings on a DVR/Hard Disk, it should also provide an on-screen Disk Usage Meter that graphically shows the user how much video is currently on the DVR/Hard Disk, along with how much space remains. Additionally, the system should have audible and visual warnings when the drive is nearing capacity.

R.1.11 - LED Indicators for Audio, Video, and Record

To ensure user awareness, the system should have LED indicators showing record, microphone, and camera activity.

R.1.12 - Saved Officer Setting

The vendor should describe how its system stores and saves user preference settings such as LCD Screen Brightness, LED Indicator Brightness, Volume, and Front Camera Auto-Zoom. These settings should be saved so that when each user logs in, his or her settings are restored.

R.1.13 - Separate Audio Channels

In order to isolate the audio during playback between the microphone(s) and the cabin microphone using a standard left/right stereo fader control, the vendor should specify audio recording system features to record the audio tracks separately. All microphones should be recorded on separate channels.

R.1.14 - Wide High Dynamic Range Camera

The vendor should specify the features in its cameras that utilize a wide dynamic range of at least 90db to create an optimally exposed image under all lighting conditions and that, at the minimum, eliminate any need for a manual backlight compensation mode for backlighted conditions (e.g., dusk or dawn, other harsh lighting conditions).

R.1.15 - Resolution

Cameras should record High-Definition video at a resolution of 1080P and/or 1280x720 (720P) with a 16:9 wide screen aspect ratio or better. Cameras should also be able to record Standard Definition video at a resolution of 864x480 (480P) with a 16:9 wide screen aspect ratio or better.

R.1.16 - Video Compression

The vendor's proposed system should have video compression features. The vendor should specify the video compression used in their BWC systems.

R.1.17 - Frame Rate

Camera equipment proposed by the vendor should have a minimum frame rate of 30 frames per second (fps).

R.1.18 - Horizontal Field of View

Camera equipment offered by the vendor should have a field of view of at least 90 degrees. The vendor is to specify the maximum field of view of its camera equipment.

R.1.19 - Camera Focus

Camera equipment should be able to focus on all objects from approximately 1 foot away to infinity. Only continuous autofocus or fixed focus devices will be accepted. The vendor is to specify any automatic image stabilization features available.

R.1.20 - Audio Capacity

Audio recording is required. The audio recording system should be capable of clearly capturing conversational speech at 3 feet without wind or excessive background noise.

R.1.21 - Low Light/Night Mode

Camera equipment proposed by vendors should be capable of recording useable video in both low light and nighttime conditions. The vendor should describe the technologies used in its cameras to improve the quality of video taken under these conditions.

R.1.22 - Synchronization

Audio recordings should be synchronized with the video captured by the camera. In addition, the camera should be synchronized in some manner with an external universal clock to ensure time accuracy.

R.1.23 - GPS

The BWC units should have GPS capabilities, and the GPS information should be embedded in recorded video.

R.1.24 - Facial Recognition

BWCs should not be equipped with facial recognition software, and the footage obtained from BWCs should not be subject to facial recognition technology, except as permitted and following the procedures established under state law.

R.1.25 - Pre-Event and Post-Event Recording

The camera should have a pre-record feature (buffer) of at least 30 seconds. The system should also be capable of automatically capturing post-event video for at least 2 minutes. The vendor should specify product features for these settings to be independently adjustable and restricted by a supervisor. Pre- and post-event times shall be continuous with the record event. Systems that record pre- and post-event times onto separate video events shall not be acceptable.

R.1.26 - Single Button

The BWC should be capable of activation and deactivation by pressing a single button.

R.1.27 - Covert/Stealth Mode

To allow the user to covertly record, the system should allow the user to quickly disable the camera's screen and LED indicators while automatically activating all audio and video recording. Vendors should describe the user safety features of their BWC solutions, such as stealth mode with lights/audible alerts dimmed and sound muted by the user.

R.1.28 - Automatic Activation

The BWC should be capable of automatic activation when triggered by accessory sensors that register when a firearm or electrical discharge weapon are drawn. The BWC should be capable of automatic activation when a paired cruiser camera system is activated. Other sensors such as those that detect sudden shocks, radio emergency button activation, or long periods of officer inactivity ("officer down") are highly recommended.

R.2 DATA STANDARDS

R.2.1 - Data Transfer

The vendor should describe, in detail, the method(s) its systems use to transfer data from the camera to the backend system. The vendor should describe wireless or Bluetooth capabilities and should also describe the ability to communicate with Mobile Data Computing (MDC) systems.

R.2.2 - Uploading

BWCs should connect to a base and upload video recordings automatically, that is, without requiring any further actions by the user. Additionally, if the BWC is powered off or if the battery is dead, the act of attaching the BWC unit to its base should power it on and automatically initiate the upload process.

R.2.3 - Data Redaction

The video management system should have audio and video redaction capabilities. The vendor should fully describe the redaction features and capabilities.

R.2.4 - Storage and Sharing

The vendor should provide a cloud-hosted solution for video storage and management. The agency should be able to control which e-mail addresses and domains are allowed to be sent links to shares, how long the shares are available, and the type and security of the share. The agency should be able to remove the share at any time. All information stored in the cloud should be stored in a "government cloud" or "government region" within a secure data center. Additionally, the audit log for the video should maintain an audit trail for the video when it is exported to the cloud and when it is viewed or downloaded.

R.2.5 - Data integrity

To guarantee data security and integrity, the system should ensure that the user cannot delete, edit, or erase original videos from any device.

R.2.6 - Video Trimming

The vendor solution should support the ability to trim video for the purpose of removing part of the video file by trimming the beginning and/or end portions of the event. The trimmed file

should be saved as a new file in order to preserve the original file.

R.2.7 - Format

Video and audio should be recorded and exported in a standard, open, non-proprietary format, including both Codec and Container, such that it can be replayed in freely available software (e.g., VLC player) without processing or conversion. Standard open formats should be used for interoperability (e.g., MP4 and MKV). Data formats that can only be viewed within manufacturer-specific replay software should not be proposed.

R.2.8 - Audit Log

Video should also be accompanied by a full audit log showing every time the event was moved, reviewed, or exported with full verification data. Exported video should include embedded date/time stamp.

R.2.9 - Metadata

Information about the event category, camera wearer/username, location, date, time, and event notation should be collected and packaged in the video format. The vendor should specify any additional metadata information captured and recorded, such as record status, microphone status, emergency lighting status, and GPS coordinates.

R.2.10 - Programmable Event, Categorization, Tagging

Camera systems should allow for event categorization and tagging by users. Categorization selections should be administratively configurable and allow selection via a pre-defined list, numeric text, or alphanumeric text input. Systems should allow the agency to program at least 4-different event category prompts in order to collect data deemed relevant regarding each recorded event. Event prompts should display automatically after each event recording has been stopped by the user. Prompts should not preclude the system from continuing to record video to its buffer.

R.2.10 - Data Retention

The vendor should provide for an agency's consideration the cost of retaining data on the cloud storage for (1) 18 months and (2) 36 months. The vendor should provide the agency with the ability to mark video and related data for cloud storage beyond the retention period.

R.3 MANAGEMENT STANDARDS

R.3.1 - Video Management

The vendor should describe, in detail, its video management solution, including all licensing and software features. Video management solutions should include searching, event marking, categorization, editing, and redacting capabilities. The vendor should also describe, in detail, how its system ensures chain-of-custody requirements.

R.3.2 - Video Dissemination

The vendor should fully describe features/options that will allow the agency to easily disseminate the video. The solution should include tracking/logging and audit capabilities associated with dissemination (e.g., date, time, sender's username, receiving agency, user information, etc.).

R.3.3 - Reporting

The vendor should fully describe its system features/capabilities for report generation by the BWC user and/or agency**.**

R.3.4 - Security-Video Review Access Permissions

If or to the extent allowed under agency policy, users should have access to their own video. However, with Supervisor or Administrator privileges (configurable), the user should be able to search and review all video on cloud storage.

R.3.5 - Security-Supervisor Controls

The BWC system should provide the ability to restrict access to all settings by way of supervisor passwords. Multiple supervisor passwords should be supported.

R.3.6 - Camera Assignments

A simple method for assigning a camera to a user should be required.

R.4. CONTRACT STANDARDS

R.4.1 - Procurement contract

An agency intending to purchase body-worn cameras should utilize the state procurement contract entitled Public Safety Equipment and Two Way Radio (PSE01).

R.4.2 - Data storage contract

Any contract for storage of body-worn camera footage shall require compliance with the Security Standards issued by the Criminal Justice Information Services, Federal Bureau of Investigation. [https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view]

RECOMMENDED REGULATION GOVERNING USE OF BODY WORN CAMERAS

R.5. OPERATION STANDARDS

R.5.1 - Commencement of Shift

At the beginning of each shift, the BWC user shall -

- Ensure that the issued equipment has a charged battery and is functioning properly;
- Notify a supervisor whenever there is a malfunction or damage to the BWC;
- Only use agency issued and approved BWC technologies; and
- Wear the BWC by mounting it on the chest, unless the stature or other physical attributes of the user, or the evolution of BWC technology, necessitate a different placement location in order to maximize the camera's ability to capture video footage of the user's activities.

R.5.2 - On-duty requirements

While on duty, the BWC user shall -

- Activate the equipment and record as specified in this policy;
- Return equipment to its dock or charging base prior to the end of each shift;
- Properly tag/classify recordings for retention;
- Document the existence of a BWC recording in written narratives; and
- It is recommended that users shall not access or view any recording of an incident involving the user before the user is required to make a statement about the incident.

R.5.3 - Docking/uploading requirements

At the end of the shift, each user shall -

- Place their BWC into a docking station. The docking station will charge the BWC's battery and transfer video data to the storage system.
- Place their BWC in a docking station no less than one (1) time per week and upload all of their video data into the evidence management system, unless otherwise directed by the Section/Station/Unit Commander.
- Ensure uploaded videos are properly tagged/classified in the evidence management system for retention.
- Before going on any planned leave of one (1) work week or more, place the BWC in a docking station and upload all of their video data into the evidence management system.
- Immediately notify the first line supervisor if the user becomes aware that this process is not occurring or becomes aware of any other malfunction of the system.

R.5.4 - Recording requirements

- BWCs shall be activated whenever a user interacts with a member of the public, including

but not limited to, when a user arrives on an enforcement or investigative scene and during any contact that becomes adversarial after an initial contact in a situation that would not otherwise require a recording, unless such activation would pose a serious threat to the user's safety or is otherwise exempted by agency policy, in which case it should be activated as soon as it is safe and permissible to do so.

- Following the activation of the camera a user should give verbal notice or otherwise make the individual[s] aware that the interaction is being recorded.
- Any recording that does not commence at the inception of the encounter, and/or is discontinued before the conclusion of the encounter, shall be explained in writing by the user. The recording shall continue to the conclusion of the incident or within the guidelines or other exceptions outlined in these recommendations.
- Applications for a search warrant shall specifically request use of a BWC during the execution of the search warrant.

R.5.5 - Notice of recording

In the event that a user seeks entry into a home, or other place where there exists a reasonable expectation of privacy, based on a justification of consent only, the user should give verbal notice or otherwise make the individual[s] aware that the interaction is being recorded.

R.6 SANCTIONS AND DISCIPLINE

R.6.1 - Failure to activate

In cases where a user does not activate their body-worn camera when policy dictates they should, the user shall indicate in their report that the BWC was not activated and the reason why.

R.6.2 - Improper use

In cases where there is an improper use of the BWC, or an individual has tampered with a recording, or improperly destroyed a recording, sanctions should be based on the progressive discipline model and be in accordance with current collective bargaining agreements.

R.6.3 - Proportionality of sanctions

Sanctions or discipline should be directly proportionate to the seriousness of the violation. For example, discipline may be less severe if the camera was not turned on for a minor citizen encounter versus if the camera is not turned on or intentionally turned off during a use of force incident.

R.6.4 - Repeat violations

Repeated violations of the agencies' BWC policies should be subject to progressive discipline, and such discipline should include penalties up to and including termination for repeated/flagrant violations of the policy.

R.6.5 - Termination

Officers terminated due to violations of the agencies' BWC policies should be referred to the Commonwealth's Peace Officer Standards and Training Commission for further action.

R.7 PROCEDURES FOR SUPERVISORY INTERNAL REVIEW AND AUDITS

R.7.1 - Supervisory review

The supervisors, managers, and command level members of an agency all shall be involved in the oversight of their BWC program. The agency should ensure that BWC-equipped users utilize the BWC in accordance with agency policy.

R.7.2 - Periodic reviews

Supervisors shall conduct periodic reviews of the BWC recordings generated by users under their command in order to assure proper functioning and use of the equipment; identify recordings that may be appropriate for agency training; and assess user performance and compliance with agency policy.

R.7.3 - Supervisory policy consideration

When exercising their BWC responsibilities, supervisors should consider:

- Inspections to ensure the BWC equipment is functional and in good order.
- Developing procedures to report malfunctions to supervisors.
- Conducting periodic reviews by supervisors/managers/command level staff to ensure recordings are properly tagged/categorized.
- Periodic review by supervisors/managers/command level staff to ensure users are complying with laws/regulations/agency policy.
- As part of supervision, any supervisory member within the BWC user's immediate chain of command should perform regular reviews and auditing of BWC usage for performance evaluation.
- Ensure that users only access BWC recordings during the course of duties in accordance with agency policy.
- Forward through their chain of command recommendations relative to BWC recordings that they believe would be worthy for user training purposes.

R.7.4 - Audits

To ensure BWC program quality and compliance, agencies should conduct audits that include:

- Compliance with agency policy on BWC utilization;
- Compliance with BWC tagging/categorization requirements;
- Compliance with BWC training requirements;
- Examination of BWC audit logs/trails for viewing/dissemination compliance

requirements; and
- Records retention compliance.

R.8 SUPERVISION AND TRAINING

The examples provided by the Task Force are not intended to be exhaustive, agency policies and collective bargaining agreements will provide further guidance on the appropriate training and use of BWCs.

R.8.1 - Personnel required to complete agency-approved training on the operation of the system and this policy

- Users who wear BWCs
- Supervisors
- Management/Command Staff
- BWC Administrators/technicians
- Records/Legal Staff/Legal counsel

R.8.2 - Scenario based policy applications

During training, the agency should present users with a number of real-world scenarios to ensure that users correctly understand how the agency's policy would apply in a particular scenario.

R.8.3 - Training providers

Training may be conducted by outside vendors, agency staff, or a combination of both. Training materials should be kept up to date by the agency and previous training materials archived.

R.8.4 - Topics for training

- Introduction and background to BWCs in policing
- Understanding video use prior to police BWCs, including:
  - Police vehicles
  - Booking facilities
  - Interview rooms
  - Private security cameras
  - Public security cameras
  - Video cameras
  - Cell phones
- Understanding the history of BWC, including:
  - When BWC use began
  - How the use of BWCs has become more common
  - What factors encourage BWC adoption

R.8.5 - Additional recommended topics for training

R.8.5.1 - Common concerns about police BWCs, including perceived benefits and risks

- Citizen privacy
- Officer privacy
- Officer safety
- Impact on citizen attitudes (satisfaction/legitimacy)
- Training and policy requirements
- Impact on officer productivity/morale
- State and federal law (public records, HIPAA, etc.)
- Logistical/resource/cost requirements

R.8.5.2 - Understanding the research on BWCs

- Findings on citizen complaints
- Findings on use of force
- Findings on complaint resolution
- Findings on arrest and citations
- Findings on cost

R.8.5.3 - BWC Device Specifications

- Familiarization with technical specifications of the BWC:
  - Video resolution
  - Video/audio file format
  - BWC field of view
  - Recording indicators
  - Pre-event recording
  - Event marking
  - Battery charging
  - Recording life
  - Charging time
  - Options such as GPS and wireless connectivity
  - Mounting options

- Key operating functions of the BWC hardware:
  - Camera controls
  - Body mounting options
  - User options/alert configurations
  - Docking station

- Identify key functionality of BWC software:

- Retrieval, storage, and management of data
- Upload/download capacity of applicable network
- Data security and encryption
- Video review application(s)
- Adding notations to recordings
- Reviewing metadata

R.8.5.4 - BWC device operations

- Activate and deactivate the BWC
- Categorizing/tagging recordings
- BWC options and special features
- Docking a BWC/uploading files
- Charging the BWC
- Care and maintenance of the BWC
- Integration with other systems such as in-car camera systems, CAD/RMS
- Using the digital evidence storage system

R.8.6 - Training on BWC Policy and Practice

The Task Force recommends that all users be thoroughly familiar with the specifics of their respective agency policies that govern the use of BWCs. The Task Force further recommends training on the following:

- Inspections to ensure the BWC is performing in accordance with the manufacturer's recommendations
- Pre/post-shift inspection
- Ensuring BWC is adequately charged
- Inspecting BWC to ensure there is no visible damage and device is in working order
- Inform supervisor of any visible damage

R.8.7 - Training on officer responsibilities

The Task Force recommends training on officer responsibilities, including the need to:

- Only use agency issued and approved BWC technologies
- Wear BWC in a manner that does not obstruct or intentionally defeat the purpose of the BWC Policy
- Activate the BWC and record as specified by policy
- Properly tag/classify recordings for retention
- Document the existence of a BWC recording in written narratives
- Prior to the end of the shift, place their BWC into a docking station to charge the BWCs battery and transfer video data to the storage system
- Ensure all uploaded videos are properly tagged/classified in the evidence management system for retention
- In the event an incident or arrest report was not created, logging in a daily administrative

journal or other equivalent agency log the circumstances and reason for the failure to properly activate.

R.8.8 - Training on internal access and review

Agencies shall train their users on when they are allowed to review the BWC recordings in accordance with agency policy and collective bargaining agreements.

R.8.9 - Training on data uploads

Whenever videos are uploaded, users shall categorize the video with the following:

- Agency case/ incident number
- Assign the appropriate category to each individual video (if not already done at time of recording)
- Additional information such as any special circumstances (e.g., use of force, critical incident)
- Location of event
- All agency reports shall reflect when a BWC was activated

R.8.10 - Data storage and retention (Agencies shall train their users on)

- Evidence/data storage access and security policy
- Agency video labels/tags/categories list
- Retention schedule of videos
- Audit logs, audit trails, or similar records

R.8.11 - Release of BWC video

- All recordings are the property of the agency, not the employee, and any dissemination shall be approved by the chief or their designee (e.g., District Attorney's office, legal section, or legal counsel).
- BWC recordings shall not be:
  - Used for the purposes of ridiculing or embarrassing any employee or person depicted on the recording.
  - Copied/filmed/photographed/reproduced in any fashion by any employee other than in the course of their official duties, and with supervisor approval.

R.8.12 - Special policy and operations considerations, such as –

- Collective bargaining agreement
- Relevant BWC case law
- Law Enforcement Body Camera Task Force recommendations
- Applicable state, federal, and local laws or regulations

R.8.13 - Supervisor training

Supervisors should receive the same base training on body-worn camera systems as users do, whether or not the supervisors will also be issued body-worn cameras. This requirement ensures that supervisors also understand the system and how it operates.

R.8.14 - Additional supervisor training

Supervisors should also receive training on supervisor responsibilities under agency policy, such as how to:

- Ensure all subordinate users are trained in proper use of BWC system
- Ensure all users assigned a BWC utilize the BWC in accordance with policy
- Ensure subordinates are made aware of policy/law updates that affect BWC use
- Ensure all users follow established procedures for the use and maintenance of BWCs
- Protocol supervisors shall follow for users with lost/damaged/malfunctioning BWCs

The supervisor should also know:

- Supervisor quality assurance duties (review to ensure proper BWC use/user performance)
- How to review BWC audit log to ensure system access compliance
- The protocol for addressing BWC policy violations
- Duties on complaint intake when there is an associated BWC recording(s)
- Policy on allowing access to subordinate's recordings
- Supervisor responsibilities for BWC evidence following a critical incident involving subordinate officer (shooting, use of deadly force)

R.8.15 - Managers/executives/command staff training

To ensure that agency Managers/Executives/Command Staff understand how the BWC operates, they should receive the same basic training on BWC as users do.

R.8.16 - Additional managers/executives/command staff training

Managers/Executives/Command Staff training should also receive training on the process for:

- Ensuring all subordinate officers are trained in proper use of BWC system
- Ensuring all users assigned a BWC utilize the BWC in accordance with policy
- Ensuring subordinates are made aware of policy/law updates that affect BWC use
- Ensuring all users follow established procedures for the use and maintenance of BWCs
- The protocol that commanders shall follow for users with lost/damaged/malfunctioning BWCs
- Quality assurance duties (review to ensure proper BWC user/officer performance)
- Reviewing of BWC audit log to ensure system access compliance
- The protocol for addressing BWC policy violations
- The policy on allowing access to subordinate's recordings
- Responsibilities with respect to BWC evidence following a critical incident involving

subordinate officer (shooting, use of deadly force)
- The protocol on exporting/sharing of BWC evidence
- The records retention policy, restricting access to BWC recordings

R.8.17 - BWC administrators/technician training

BWC Administrators/technicians should receive the same base training on body-worn camera systems as users do, to ensure that the BWC Administrators/technicians understand the system and how it operates.

R.8.18 - Additional topics for training for administrators/technicians

- BWC Organization management (agency information, security groups/roles and permissions)
- BWC Evidence Storage management (system monitoring, evidence retention rules, archiving, auditing)
- BWC Device management (device configurations, create and maintain event categorizations, software updates, hardware assignments, maintenance, and troubleshooting)
- Microsoft, Linux, and Mac OSX operating, and file systems as used by the agency, related desktop applications and server applications
- Networking (TCP/IP, organization network schema, switch/router/firewall operations and configuration)
- Agency inventory procedures
- BWC troubleshooting and basic repair of system components
- BWC contract and warranty provisions and procedures
- End user training

R.8.19 - Records/Legal Staff Training

Records and legal staff or legal counsel utilized by the agency should receive the same basic training on body-worn camera systems as users do, to ensure that the records and legal staff understand the system and how it operates.

R.8.20 - Additional Training for Legal and Records Personnel

Training on topics necessary to respond to evidentiary and Massachusetts Public Records Law (G.L. c. 4, § 7(26)) requests, such as:

- Federal and Commonwealth rules of evidence and disclosure, responding to FOIA requests, pertinent privacy laws, records retention regulations
- Procedures used by the agency to respond to public records request
- Software applications related to collection, storage, organization, security, redaction, reproduction and dissemination of agency body worn camera videos
- Agency tracking system for providing video evidence to requesting parties to fulfill

freedom of information requests
- Use of software productivity suite applications (word processor, spreadsheet, email)
- Video editing software use (commercial products or BWC vendor system)

R.9 - <u>STORAGE, MAINTENANCE, AND HANDLING</u>

R.9.1 - Identification

All recordings shall be identified by date, time, location, incident number, type of incident, and assigned user.

R.9.2 - Storage standards

BWC footage shall be stored in compliance with the Security Standards issued by the Criminal Justice Information Services, Federal Bureau of Investigation.

R.9.3 - Procedures to protect integrity of BWC recordings

Every agency shall establish and maintain a system and procedures to ensure the integrity, proper handling, and storage of all BWC recordings. This system shall include provisions to:

- Ensure that all recordings are uploaded to a secure data storage system in a timely fashion;
- Prevent tampering with or deletion of recorded data both before and after downloading from the BWC and uploading to the storage system;
- Prevent unauthorized access to stored BWC recordings;
- Document all instances where BWC recordings are accessed, viewed, copied, disseminated, or deleted; and
- Permit auditing of all instances where BWC recordings are accessed, viewed, copied, or deleted.

R.9.4 - Locating Specific BWC Recordings

Every agency shall establish and implement a system that permits the agency to locate and retrieve all recordings associated with a specific incident/event, investigation, case, or criminal charge. Accordingly, every agency shall be required to develop and maintain a BWC control ledger or log, which may be computerized. Every agency shall establish and implement a system to ensure that relevant BWC recordings are provided in discovery in a timely fashion. The system established by the agency should include a provision to ensure that police arrest/incident/continuation reports indicate whether the incident or investigative activity described in the report was electronically recorded by a BWC. Police reports should, when feasible, indicate the corresponding BWC control ledger/log number, and the BWC control ledger/log should cross-reference the incident case number if one is available. Copies of BWC recordings made for the purpose of complying with the Commonwealth's discovery obligations shall be provided to the prosecutor in a commonly available media format.

R.9.5 - Provisions to identify recordings that raise special privacy or safety issues

To identify BWC recordings that may raise special privacy or safety issues, every agency that deploys BWCs shall establish and implement a system that permits an event notation to be made when the recording:

- Captures the image of a victim of a criminal offense that may have privacy or safety concerns;
- Captures the image of a child under the age of 18;
- Was made in a residential premises (e.g., a home, apartment, college dormitory room, hotel/motel room, etc.), a school or youth facility, a healthcare facility or medical office, a substance abuse or mental health treatment facility, or a place of worship;
- Captures a conversation with a person whose request to de-activate the BWC was declined;
- Captures a special operations event or execution of an arrest and/or search warrant where confidential tactical information (e.g., verbal codes and hand signals used to give direction to officers, techniques for interior movements and clearing rooms during execution of a warrant, techniques for convincing persons to open doors during warrant execution, etc.) may have been recorded;
- Captures the image of an undercover officer or confidential informant; or
- Captures the screen of a police computer monitor that is displaying confidential personal or law enforcement sensitive information.

Such notation shall be permanently attached to the recorded event. Before any release of a recorded event with a special privacy or safety issue notation, the event shall be reviewed by the agency's appropriately trained staff to properly assess those issues, and if necessary, the recorded event shall be redacted accordingly before release.

R.9.6 - Release of a BWC recording that is the subject of an active criminal investigation or prosecution.

Approval for release of a BWC recording that involves the subject of an active criminal investigation or prosecution shall comply with the public records law.

R.9.7 - Compliance with discovery obligations relating to BWC recordings that might expose officers or other persons to danger.

If disclosure of a BWC recording as part of the Commonwealth's discovery obligations in a prosecution might present a danger to any officer or civilian (e.g., reveal an undercover officer, confidential informant, surveillance site, etc.), or might reveal confidential tactical information the disclosure of which might jeopardize future operations or officer safety (e.g., verbal codes or hand signals used to communicate information or instructions, techniques for interior movements and clearing rooms during execution of warrant, techniques for convincing persons to open doors during warrant execution, etc.), the Attorney General/District Attorney of

jurisdiction or designee, shall, in the exercise of sound prosecutorial discretion, take such steps as are appropriate and authorized by law and/or court rule to protect the information from disclosure, such as by seeking a protective order from the court.

R.9.8 - Third-party storage and maintenance

If a law enforcement agency authorizes a third party to act as its agent in maintaining recordings from a BWC, the agent shall be prohibited from independently accessing, viewing, or altering any recordings, except to delete recordings as required by law or agency retention policies.

R.9.9 - Including BWC data in a public record

The release of video recording data and metadata as a public record and shall only be done in compliance with the Commonwealth's public record laws and regulations, and all applicable state and federal privacy statutes.

R.10 - <u>RETENTION</u>

R.10.1 - Length of Retention

The agency shall retain all BWC recordings for not less than 180 days but no more than 30 months, unless otherwise required under the retention schedule for municipalities established by state law, or the Office of the Secretary of State, which may be found on the Secretary of State's website.

> The Task Force notes that the "not more than 30 month language" stipulated by the legislative language conflicts with the statute of limitations for civil cases (3 years) and that consideration should be given to changing it to 37 months. In addition, the "not less than 180 days" stipulated by the legislative language does not allow sufficient time to determine whether recordings need to be accessed and consideration should be given to changing it to one year.

R.10.2 - Destruction of recordings

No BWC recordings shall be deleted/destroyed while any related investigation, including criminal, civil, or administrative investigation, or court proceeding is still open/pending, or for the same period of time that evidence is retained in the normal course of the investigation, or for the same period of time that evidence is retained in the normal course of the court's business for a recording related to a court proceeding. Similarly, no BWC recordings shall be destroyed until all appeals and/or related litigation is exhausted and closed.

R.10.3 - Retention for litigation

In cases in which a recording has been requested for litigation, the District Attorney's Office and/or the agency's legal section shall be notified of the request and said request shall be

addressed pursuant to evidentiary rules of court.

R.10.4 - Prosecutorial and court ordered restrictions

Access to BWC recordings are subject to all state and federal laws, and any orders of a court of competent jurisdiction. BWC recordings shall be preserved, stored, and retained in accordance with the requests, directions, and orders of appropriate prosecutorial and/or judicial authorities.

R.10.5 - Security of storage facilities

Storage of BWC data shall be consistent with the standards established by the Federal Bureau of Investigation's Criminal Justice Information Services. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view.

Respectfully submitted,

Angela F.F. Davis, Chair
Assistant Undersecretary for Law Enforcement and Criminal Justice
Executive Office of Public Safety and Security
617.620.8544
Angela.f.davis@state.ma.us

Major Steven McCarthy
Division of Homeland Security and Preparedness
Massachusetts State Police
508-867-1052
steven.mccarthy@pol.state.ma.us