Security Protective Service Body-Worn Cameras

Issue Date: 12/19/2023

1. Purpose

1-1 This policy establishes guidelines for the proper use, management, storage, and retrieval of audio and video media recorded by body-worn cameras (BWCs). This policy applies to all SPS officers within the United States who are exercising law enforcement authorities authorized under Section 15 of the CIA Act, 50 U.S.C. § 3515, and those who the program administrator has approved to use a BWC.

2. Definitions

2-1 *Activate*. Physically pressing the appropriate button on the BWC that will begin a recording. This action will also capture the previously buffered recording of the encounter.

2-2 *Body-Worn Camera*. A device issued by SPS and worn on an individual officer's person that records and stores audio and video.

2-3 *Buffering*. The option to let a BWC pre-record before activation of the device.

2-4 *BWC Program Administrator*. The SPS program administrator for digital storage and the camera system who has full access to user rights and sets user access and parameters.

2-5 *Case ID*. The numeric identifier that can be attached to the BWC videos. This will be the SPS electronic Computer Automated Dispatch (CAD) case number.

2-6 *Critical Incident*. An incident in which an officer observes or is involved in potentially life-threatening circumstances, use of force, or when any person suffers serious physical injury.

2-7 *Deactivate*. Physically pressing the appropriate button on the BWC that will end the recording.

2-8 *Digital Evidence Management System (DEMS)*. A Software as a Service platform to store and manage digital evidence.

2-9 *Digital Recordings*. BWC files, including photographs, audio recordings, and video footage or other data, captured by a BWC and stored digitally in accordance with the applicable CIA Record Control Schedule (RCS).

2-10 *Docking Station*. A portable multi-ported docking station installed at each station that simultaneously recharges the BWC while uploading all digital data from the BWC. The docking station then transfers the digitally encrypted data to the DEMS.

2-11 *Inadvertent Recording*. Any non-volitional, unintentional recording or any recording that does not comply with this policy or applicable law.

2-12 *Officer*. Any SPS member authorized by SPS to wear a BWC.

2-13 *Public*. Any individual who is not employed by or otherwise affiliated with the CIA.

2-14 *Serious Bodily Injury*. Injuries that create a substantial risk of death, unconsciousness, extreme physical pain, disfigurement, fractured or dislocated bones, or loss or impairment of the function of a bodily member, organ, or mental faculty.

3. Policy

3-1 SPS officers must utilize BWCs in accordance with both this policy and Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety." BWCs can build public trust by providing transparency and accountability in circumstances where the use of force may reasonably be anticipated.

3-2 Officer safety takes precedence over BWC operation. Officers must not allow the operation of BWCs to interfere with their personal safety or the safety of others.

3-3 Only authorized officers may possess or use a BWC.

3-4 Officers may use only a CIA-issued BWC.

3-5 Officers may use a BWC only in the performance of official police duties and not for personal purposes.

3-6 Officers must maintain their assigned BWCs in working order, charged, and with enough data storage capacity to complete their shift under normal circumstances.

3-7 An officer wearing a BWC must place the device so that it is above the midline of the torso and maximizes the camera's ability to capture video footage of the officer's activities.

3-8 Officers must operate BWCs with the buffer activated and set to 30 seconds, unless the officer is working in an administrative capacity where contacts with the public are unlikely.

3-9 Officers must not alter, remove, dismantle, or tamper with any hardware, software component, or other part of the BWC. Nor must any BWC digital evidence be deleted or altered in any manner, unless explicitly authorized by this policy.

3-10 Officers are not required to announce or otherwise inform members of the public that their BWCs have been activated. However, officers may find that such a notification can be an effective tool to de-escalate. If asked by a subject, officers should advise they are being recorded.

3-11 Officers must not wear or otherwise transport BWCs into CIA buildings, absent extraordinary circumstances where the safety of officers or CIA personnel is at risk (e.g., in pursuit of a subject into a CIA building).

3-12 Officers will follow all relevant Agency regulations regarding data collection and privacy [redacted].

3-13 Accessing, copying, forwarding, or releasing any recording other than for official use, and contrary to these procedures, is strictly prohibited.

3-14 Personal computer equipment and software programs must not be utilized when making copies of digital evidence. Using a personal recording device such as video camera, cell phone, or other device to record or capture digital evidence from a BWC device or digital evidence storage is strictly prohibited.

3-15 BWC use does not diminish the requirement that officers document their activities and observations through detailed police reports. A police report remains the appropriate place to document the totality of the circumstances of the incident.

3-16 Any failure to have the BWC activated per this policy must be documented in CAD notation and a police report.

3-17 BWC digital evidence may be subject to public release in accordance with this policy and federal law. Consistent with applicable law, expedited release may be appropriate where the incident involves death or serious bodily injury.

3-18 Violations of this policy will be handled in accordance with Agency regulations and SPS policy and may be subject to disciplinary action.

3-19 Specific questions relating to this operational order should be directed to your immediate supervisor or regional commander.

4. Training

4-1 Officers must complete BWC training prior to using any BWC. Training includes but is not limited to legal implications regarding BWC use, practical use issues, evidentiary continuity, technical elements, sensitivity issues, and professional standards.

4-2 In order to use a BWC, officers must have completed privacy and civil liberties training per Agency requirements.

5. Pre-shift Inspection

5-1 Prior to the beginning of each shift, an officer assigned a BWC must inspect the device to ensure that it is properly performing. This inspection includes confirming that the battery is adequately charged and that the BWC is free from debris.

5-2 Any malfunction or error indicators must be reported to a supervisor as soon as practical. If any BWC equipment is determined to be inoperable, it will be taken to the program administrator for repair by the manufacturer or a certified repair vendor as soon as possible.

Inoperable equipment will be tagged and returned to the program administrator as soon as possible.

6. Activation

6-1 Recognizing that officers could be surprised by a dynamic event, BWC activation is required only when it can be safely done.

6-2 Officers will activate their assigned BWC when:

A. conducting any kind of law enforcement search (consensual or otherwise);
B. making an arrest;
C. transporting a prisoner; or
D. approaching a subject as part of a pre-planned arrest.

6-3 Recording should be incident-specific; officers should not record their entire shift.

6-4 When an officer fails to activate the BWC, fails to record the entire contact, or interrupts the recording, the circumstances will be documented in the CAD and in the associated police report.

7. Deactivation

7-1 When a BWC has been activated, it must not be deactivated until the incident has concluded, unless

A. the officer has reason to believe that the incident is of such lengthy duration that deactivation is necessary to conserve recording times;

B. the officer enters a location where the individual has a reasonable expectation of privacy (e.g., a restroom); or

C. the officer utilizes discretion to stop recording a sensitive situation, which may include protection of classified information.

7-2 The officer will verbally indicate their intent to stop recording and the reason before deactivating the BWC. The officer will also do so before reactivation, if applicable. To avoid starting and stopping recordings, officers should consider using the mute function when appropriate (e.g., to consult with another officer). Officers should give a verbal indicator prior to stopping the recording, or using the mute function, to avoid the misconception that the audio was malfunctioning when later reviewed.

8. Prohibitions

8-1 Officers must not activate their BWCs in the following circumstances:

A. When inside CIA buildings, unless extraordinary circumstances are present, which may include responding to a use of force incident or a felony crime of violence;

B. Recording areas or activities such as pre-shift conferences, locker rooms, break rooms, or other activities not related to a criminal investigation;

C. Recording third parties who are not relevant to the underlying purpose of the investigation;

D. In a facility whose primary purpose is to provide medical or psychiatric services, unless the officer is escorting a subject, or riding with emergency medical services transporting a subject to this type of facility; in this instance, officers must be aware of patients' privacy rights when in hospital settings and must endeavor to avoid recording persons other than the suspect; or

E. Minors should not be recorded without their parent's consent when they are not a suspect or victim. In circumstances where minors are incidentally recorded, their images may be concealed during the redaction process if necessary.

9. Inadvertent Recordings

9-1 Any inadvertent recording will be deleted. The program administrator will make this determination in writing.

10. Data Upload

10-1 Officers must follow the BWC manufacture's guidance in the operation of charging stations and any other peripherals used to upload data to the DEMS. Uploads should be done once per shift. Officers must add case IDs to the DEMS for video files that are associated with those case numbers. Officers must assign all video files to an appropriate category prior to, or after, being uploaded to the DEMS. The categories are as follows:

A. *Evidence*. Evidence of crime is on the video, and an arrest or mandatory appearance citation occurs. This would also include any use of force incident or where an incident results in death or serious bodily injury.

B. *Non-evidentiary.* General law enforcement incident without a citation issued or arrest made.

C. *Citation issued.* General law enforcement incident with a case number assigned and an optional citation issued. An example of this would be a basic traffic stop with an optional citation issued.

11. Critical Incidents

11-1 Following a critical incident, all involved officers will turn their BWCs over to a supervisor on scene prior to viewing any recording of the incident. The receiving supervisor is responsible for uploading the BWC data in a timely manner. No officer present at the scene of a critical incident may review a recording of a critical incident until authorized by a supervisor and with the concurrence of the regional commander and the Office of General Counsel (OGC).

12. Digital Evidence Review

12-1 Digital evidence captured by the BWC is not all-inclusive. The system captures a less broad and less detailed image than the totality of the human senses. An officer's recollection of specific details may be different from what is captured in digital evidence. Unless prohibited by Section 11, or otherwise directed by OGC or an Assistant US Attorney or other prosecutor, officers should review digital evidence prior to completing reports, providing testimony as a government witness at a hearing, trial, or deposition.

12-2 Digital evidence may be reviewed as part of an internal administrative investigation.

12-3 Digital evidence should not be reviewed for the purpose of general performance review or for routine preparation of performance reports.

13. Expedited Recording Release to the Public

13-1 Expedited public release of BWC digital recordings is generally required as soon as practicable, if permitted by law, where the incident involves serious bodily injury or deaths in custody. The release of such recordings must be coordinated with OGC. Such release must also be consistent with applicable law, including the Privacy Act of 1974, and must take into account the need to promote transparency and accountability, the duty to protect the privacy rights of persons recorded, the need to protect ongoing law enforcement operations, and the obligation to protect intelligence sources and methods. Redactions may be applied to BWC digital recordings prior to release, consistent with applicable law and in coordination with OGC.

14. Recording Retention

14-1 All videos made by BWCs will be uploaded to the DEMS. Digital evidence captured by BWCs must be treated as official records and handled consistent with existing Agency regulations and federal law.

14-2 All recorded images and audio recordings are the property of the CIA and must be treated in accordance with CIA's applicable RCS or as non-records for inadvertent recordings that have no value to the CIA. In addition, recordings that are categorized as evidence under section 10-1, as well as recordings that may relate to any pending or anticipated criminal investigation or prosecution, civil litigation, administrative proceeding, FOIA matter, or congressional oversight activity, and that are subject to a legal hold, must be retained and may not be destroyed until the legal hold is removed or the office that placed the hold approves.

15. Digital Evidence Control

15-1 Digital evidence related to possible criminal charges must be treated the same as other forms of direct evidence per SPS policy. This evidence must be made available to the prosecutors and may be subject to legal disclosure requirements. Such evidence and all other recordings requiring retention under Section 14 must be provided to the Court Liaison Office (CLO) for storage and transfer in order to protect the integrity of such evidence. In order to comply with the law, the CLO will alert the prosecutors of all BWC recordings when such recordings pertain to a criminal case, and the CLO will notify OGC in all cases.

16. Supervisor Responsibilities

16-1 It is incumbent on all supervisors to ensure officers have access to operational BWCs and utilize BWCs according to this policy. Supervisors must ensure the appropriate recordings are restricted and that recording officers do not review the recording of any critical incident. SPS management (lieutenant or higher) may review footage related to complaints made against an officer.