



# Office of the Inspector General

## SOCIAL SECURITY ADMINISTRATION

### **BODY-WORN CAMERA PROGRAM<sup>1</sup>**

- A.** The policy outlined in this Section pertains to the devices that are worn overtly on the outside of a Special Agent's clothing or equipment.
- B.** The Office of Investigations (OI) will provide body-worn camera (BWC) systems to SAs to (1) provide an additional layer of safety for the SA, (2) build trust in the communities OI serves by adding transparency and accountability in law enforcement operations, and (3) record interviews, obtain statements, or otherwise secure evidence in connection with an investigation.
- C.** Only OI SAs and law enforcement agents or officers assigned to Cooperative Disability Investigations (CDI) units (CDIUs) may use BWCs under OI authority.
  - 1.** OI SAs will use only those BWCs that have been sourced and provided by OI headquarters (HQ). These BWCs possess features and functionality specific to this policy, and other devices procured by OI field offices may not be used under the authority of this Section.
  - 2.** CDI law enforcement agents and officers must overtly use the BWCs issued by their employing agencies for CDI investigations when engaging in the mandatory-use activities outlined in Subsection F. below in CDI investigations. Sworn officers assigned to CDI units who have plans to engage in the mandatory-use activities outlined in F. below in CDI investigations, and who do not have a BWC, will make use of a CDI-provided BWC.
  - 3.** Personnel are not permitted to use personally- or privately-owned devices as a BWCs.
- D.** OI's BWC program is managed by the BWC Program Manager. The BWC Program Manager is responsible for, among other things, ensuring that OI SAs have the necessary hardware and training to implement this policy, developing and updating BWC training material, advising the Policy and Compliance Team regarding updates to this policy, acting as OI's point of contact with the BWC vendor, and serving, when requested, in an advisory role to OIG's executive team when questions arise about the redaction and release of BWC footage.
- E.** Before the carriage and deployment of a BWC, personnel must be trained in the device's use, pursuant to an OI-approved training course, and the policies outlined in this Section. Prior to using the device for the first time, SAs will ensure that the training is properly accounted for in OIG's training database.

---

<sup>1</sup> This policy was issued on August 23, 2022 in accordance with the executive order on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (EO 14074), and advances and enhances existing BWC policy. Full implementation and effectuation of this text is delayed until after the procurement of BWC equipment and training.

1. In addition to the initial required training, SAs must also complete an annual familiarization course developed by the BWC Program Manager. This training will be completed in conjunction with officer response tactics or firearms training. If an SA is unable to complete the required training, they will seek alternate training from the BWC Program Manager through their supervisor. SAs may also receive refresher BWC training during in-service training.
2. CDI law enforcement agents and officers will receive training on their issued devices in accordance with their employing agency's policies and are not required to participate in OI's approved BWC initial or recurring training courses. They are however, before using their BWCs in CDI investigations, required to review this policy and acknowledge understanding of it, in writing, to the division Special Agent in Charge (SAC) through their chain of command.
3. CDI law enforcement agents and officers making use of a CDI-provided BWC will comply with the BWC training requirements established for OI SAs.

**F. Mandatory Use of Body-Worn Cameras: Enforcement Operations**

1. In concert with the *Body-Worn Camera Policy* issued to Department of Justice agencies by the Office of the Deputy Attorney General in June 2021, and in accordance with the requirement set forth in the executive order on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (EO 14074), OI SAs will wear and activate BWC recording equipment for purposes of recording their actions during each of the following:
  - a. Pre-planned attempts to serve an arrest warrant, or other pre-planned arrests, including the apprehension of fugitives sought on state and local warrants;
  - b. Execution of search or seizure warrants or orders, to exclude searches that are not physical in nature.
2. During the pre-operation briefing, the team leader will discuss the planned use of BWCs and review the requirements of this Section.
3. Any planned deviation from OI's BWC policy must be approved, in writing, by the Assistant Inspector General for Investigations (AIGI) or their designee.
4. When conducting enforcement operations with a partner law enforcement agency that will deploy BWCs during the operation, OI personnel will comply with OI BWC policy. Prior to any said operations, the OI division SAC overseeing the operation will notify the AIGI through the appropriate Deputy AIGI (DAIGI) of any unresolved conflicts with any partner law enforcement agency regarding BWC deployment during the operation.
5. If applicable, special care should be taken to resolve any issues related to undercover agents involved in enforcement operations (see SAH 007.065(I)(9)).

6. *Internal Authority:* SAs need not seek distinct supervisory authority to use BWCs in these cited enforcement operations.

**G. Optional Use of Body-Worn Cameras: Interviews**

1. The subjects of interviews maintain the right not to be recorded in areas where they have a reasonable expectation of privacy (REP). If the interview is set to take place where the interviewee has REP, and they ask not to be recorded, the SA should explain the value of a recorded interview. If the respondent insists, the SA will deactivate the BWC and determine a course of action appropriate for the circumstances, and which is in accordance with policy and law (e.g., terminate the interview and depart the area, continue the interview using notes and without an activated BWC, move the interview to an area without REP, etc.).
2. *Internal Authority:* SAs need not seek distinct supervisory authority to use BWCs in interviews.

**H. Optional Use of Body-Worn Cameras: Other Instances**

1. In areas without REP, SAs may activate their BWC during any encounter with the public, while engaged in official business, when they believe that a video record of their activity, or that of others, may be of value to their investigation or operation, or potential investigation of a complaint against them or another SA. In these instances, SAs will, as quickly as it's practicable, alert those in the vicinity of the recording (see 007.065(I)).
2. In areas with REP, SAs will not activate their BWC without consent unless their encounter with the public decays (e.g., the public's behavior becomes erratic, violent, or assaultive, whether verbal or physical) to the point that the SA reasonably believes that their encounter may lead to the use of force of any kind, or to the filing of a complaint against them. In these instances, SAs will, as quickly as it's practicable, alert those in the vicinity of the recording (see 007.065(I)). When a person with REP objects to the recording, the SA will, when it is safe to do so, depart the area and stop recording, unless the circumstances suggest that the person should be seized.
3. *Internal Authority:* SAs need not seek distinct supervisory authority to use BWCs in other instances.

**I. When using a BWC, SAs shall:**

1. Be responsible for its protection and safekeeping. SAs shall also be responsible for maintaining the device in accordance with the manufacturer's standards, and will report any issues, or the loss or theft of a BWC, to their immediate supervisor. As necessary, the supervisor will coordinate repairs to, or replacement of, the device with the BWC Program Manager.
2. Fully charge, inspect, and test the BWC prior to each deployment to verify that the device is working properly. The SA will notify their supervisor of any problems.

3. Wear the BWC openly, in a prominent position on their body or clothing, and in a manner that maximizes the camera's ability to capture video footage of the SA's activities.
4. When use of the device is mandatory (see Subsection F. above), activate the BWC prior to contact with any persons, unless circumstances prevent recording at the beginning of an event, in which case the SA shall begin recording as soon as possible.
5. State, immediately upon activation of the BWC, "Body camera activated" or something similar, and when appropriate, identify themselves and other persons present, as well as the date, time, and any other relevant information.
  - a. During an enforcement operation (see Subsection F. above), when more than one SA will be wearing and activating a BWC, activation will occur at the direction of the team leader. The team leader will ensure that each member of the enforcement team has activated their BWC prior to beginning the enforcement action. Team leaders will generally choose to activate BWCs upon the team's approach of a subject or the premises to be searched. At the user's discretion, BWCs may also be activated when the user encounters an individual who is uncooperative, violent, assaultive, or discussing criminal conduct that in the SA's judgment, consistent with the SA's training and experience, could lead to use of physical or deadly force or be relevant to the investigation.
6. Ensure that, as soon as practical, all parties present are notified that the BWC is activated and all activities, both sight and sound, are being recorded (e.g., "Ma'am/Sir, I am advising you that our interaction is being recorded."). SAs shall repeat the notification, if practical, for additional parties that become involved in the recording.
7. Not stop the recording, absent unusual circumstances, until the conclusion of the event and departure of the immediate area. In all cases and when possible, prior to terminating the recording, SAs will state the date, time, and reason for the BWC's deactivation.
  - a. In enforcement operations generally, the deactivation of the BWCs will happen at the direction of the enforcement operation's team leader. The team leader will use their discretion to determine whether team members participating as outside cover, when applicable, should continue to record.
  - b. If executing a search warrant, the recording shall conclude when the team leader determines that the location to be searched is secure, all subjects have been searched, if applicable, and the likelihood of the use of force is minimized. For purposes of this policy, *secure* means that the scene is safe and under law enforcement control.
  - c. When executing an arrest warrant or arresting an individual during the execution of a search warrant, the operation's team leader may authorize the deactivation of most BWCs once the scene is secure (see Paragraph b. above) and any arrestees are handcuffed and placed in the transport

vehicle. SAs tasked with monitoring an arrested individual or the transport of a prisoner from the scene of an arrest, must wear their BWCs and leave them activated until arrival at a processing or detention center.

- d. Because of the limited battery life of BWCs, the enforcement operation's team leader may authorize deactivation of the devices to conserve power, if necessary. Deactivation must be deliberately timed to maximize recording of crucial evidence.
  - e. An SA may deactivate their BWC to obtain medical attention for either themselves, another SA, or a law enforcement partner.
- 8. Not record other agency personnel during routine, non-enforcement-related activities unless recording is required by court order, is authorized as part of an administrative or criminal investigation or is part of a BWC training exercise.
  - 9. Not record conversations with confidential informants (CIs), confidential sources (CSs), undercover SAs, with other law enforcement officers discussing tactics or strategy, or in public places where REP is generally given (e.g., restrooms, medical facilities, locker rooms, other places where individuals are reasonably expected to be in a state of undress).

## J. Storage of BWC Recordings

### 1. Cloud Storage for OI SAs

- a. BWC recordings will be uploaded as soon as is practicable, usually within 48 hours, and stored using an OI-approved and -controlled cloud storage service. If the upload cannot be completed within 48 hours, the SA will notify a supervisor within their chain of command of the delay and the reason for the delay. This may be accomplished via email.
- b. SAs are responsible for uploading recorded data from the BWC, except when the data involves an officer-involved shooting, in-custody death, or other incident involving an officer that results in a person's bodily harm or death. In these circumstances, the supervising Assistant Special Agent in Charge (ASAC) or Resident Agent in Charge (RAC), shall immediately take possession of the BWC and upload the data. If an ASAC or RAC is not reasonably available or was involved in the incident in question, a senior, on-site SA will act in the ASAC or RAC's stead.
- c. All BWC recordings must be properly maintained. They are the property of the OIG, and their release is governed by the same disclosure, retention, and in the case of evidence, chain of custody considerations, that apply to all other agency information. SAs should refer to SAH 007.065(L), SAH 006, SAH 014, and SAH 019 for additional guidance on these topics.
  - I. Within the cloud storage service, each BWC recording will be assigned to a case, and each case will be numbered to match the Titan-generated case number.

- II. SAs will not change the default file name created by the cloud storage service (i.e., the file naming requirements outlined in SAH 003.090 do not apply to files uploaded and stored in the OI-approved and -controlled cloud storage service).
- III. Within 10 days of a recording's upload to the cloud service, each BWC recording will be assigned one of the following retention categories:
  - (a) "Significant Investigation" is applied to those recordings acquired as part of an investigation that meets the definition of a significant investigative case file (see Chapter 5 of the *Administrative Policies and Procedures Manual* (APPM)). These files may be of probative value to either the activity under investigation or to an incident from which litigation or criminal prosecution is likely or a reasonable possibility, to include all officer-involved shootings, in-custody deaths, or other incidents involving an officer that results in a person's bodily harm or death (e.g., any use of force incident);
  - (b) "Non-Significant Investigation" is applied to those recordings acquired as part of an investigation that meets the definition of a non-significant investigative case file (see APPM, Chapter 5). These files may have probative value to either the activity under investigation or to an incident from which litigation or criminal prosecution is likely or a reasonable possibility, to include all officer-involved shootings, in-custody deaths, or other incidents involving an officer that results in a person's bodily harm or death (e.g., any use of force incident);
  - (c) "Files Unassociated With An Investigation" is applied to those recordings that are produced during any testing of or training with the device, or any other circumstance, and which do not meet the requirements established in (a) or (b) above. These files will be retained for seven days.
- IV. No BWC recordings will be deleted from any location except in accordance with applicable retention policies and only by an automated process, the parameters of which are set by OI, within the cloud storage service, or by the BWC Program Manager. The AIGI, in consultation with counsel, may approve, in writing, the deletion of BWC recordings for other reasons.
- d. Files uploaded from the BWC to the OI-approved and -controlled cloud storage service will be hashed by the cloud service (i.e., these files need not be hashed by OI SAs).

## 2. On-Premises Storage for CDI Law Enforcement Partner BWC Recordings

- a. In the event a CDI law enforcement agent or officer uses their employing agency's BWC as part of a CDI investigation, the recordings will be



handled in accordance with their employing agency's policies. Thereafter, any of these BWC recordings that are deemed to have evidentiary value to OI, as defined in SAH 007.065(J)(1)(c)(III)(a) or (b) above, will be handled in accordance with the requirements of SAH 014.

**K. Documenting the Use of a BWC**

1. SAs will note the existence of a BWC recording when documenting their investigative activity on Form OI-4, Report of Investigation. The report should document the number and names of video files created and retained for each investigative activity.
2. Any unplanned deviations from OI's BWC policy (e.g., device malfunction, operator error) shall be documented in Form OI-4, Report of Investigation, and shall address why the recording was not made, why the recording was interrupted, or why the recording was terminated.

**L. Requests For and Disclosure of BWC Recordings**

1. BWC recordings may be subject to release pursuant to the Freedom of Information Act (FOIA). Any request for records made pursuant to FOIA will be handled in accordance with SAH 019. In preparing FOIA responses, redactions will be made by the BWC Program Manager after and in consultation with the Office of the Counsel to the Inspector General (OCIG). Where appropriate, in matters of significant interest, the BWC Program Manager may also consult with the AIGI.
2. Notwithstanding the prohibition in SAH 019.010 against the release of "any records in connection with an ongoing investigation," the Inspector General may release BWC recordings, even expeditiously, when they judge that doing so best suits the demands of any given circumstance. Any discussion regarding the release of BWC recordings will include a review of the recording and evaluation of the appropriacy of redacting part(s) of it.
3. To promote transparency and accountability, and in accordance with the executive order on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (EO 14074), BWC video footage involving incidents of serious bodily injury or deaths in custody, consistent with applicable law, including the Privacy Act of 1974, shall be expeditiously released to the public by the AIGI upon consultation with the BWC Program Manager, Chief Counsel to the Inspector General, and the Inspector General. To protect the privacy rights of persons depicted in the footage, as well as any ongoing law enforcement operations, the AIGI, after seeking counsel from OCIG and the Inspector General, may direct the BWC Program Manager to sanitize the footage prior to its release.
4. BWC recordings may also be released pursuant the guidance outlined in SAH 006. In considering this type of disclosure, SAs must give thought to the redaction requirements outlined in Paragraph M. below.

#### **M. Redacting BWC Recordings**

1. In any situation in which BWC footage should not be shared because of law enforcement sensitivities, privacy concerns, or other reasons (e.g., the recording depicts undercover personnel, CIs or CSs, minors, injured or incapacitated individuals, sensitive locations), SAs may, after consultation with their immediate supervisor, their SAC, and OCIG, use redaction software to blur images or portions of images, or minimize audio content, when disclosing BWC recordings. The BWC Program manager may assist with redaction as necessary.

#### **N. Reviewing BWC Footage**

1. SAs may review a recording to refresh their recollection while preparing to make a statement, testify, or draft reports or other official documents, even if such activities are part of an SA's defense. Reviewing a recording for any other purpose must be approved by management. SAs are prohibited from tampering with or deleting BWC recordings. SAs are also prohibited from accessing recorded data for personal use and from uploading recorded data to public and social media sites. Without a legitimate business purpose, SAs are also prohibited from making copies of BWC recordings.
2. An SA's supervisory chain, and other appropriate OIG personnel, may review BWC recordings to investigate a complaint against an SA or an incident in which the SA was involved, or to identify footage for training and instruction. Division SACs, as well as an SA's ASAC or RAC, may further review BWC recordings to ensure accuracy and quality in reports detailing the activity captured by a BWC. In like manner, CDI Team Leaders may, for purposes of quality assurance, also review recordings of their law enforcement agents and officers. BWC recordings may be reviewed in other circumstances with AIGI approval.
3. Supervisors may not use BWC recordings as evidence to support a negative performance appraisal.