

LAW ENFORCEMENT AUTHORITIES

Body-Worn Cameras

APPROVAL/TRANSMITTAL

This Standard Operating Procedure (SOP) supplements directive IG-8476. It provides guidance on implementing policy concerning the use of body-worn cameras (BWC) by U.S. Department of Agriculture (USDA), Office of Inspector General (OIG) Criminal Investigators/Special Agents and other authorized personnel. This SOP contains all procedural aspects of directive IG-8476, Body-Worn Cameras, dated August 31, 2022.

---

KEVIN M. TYRRELL  
Assistant Inspector General for Investigations

---

**TABLE OF CONTENTS**

A. PURPOSE ..... 3

B. INTRODUCTION ..... 3

C. GUIDANCE FOR OIG Criminal Investigators ..... 3

D. DEPLOYMENT OF BWCs FOR ENFORCEMENT OPERATIONS ..... 3

E. BODY-WORN CAMERA OPERATION ..... 5

F. PLACEMENT OF THE BWC..... 6

G. GUIDANCE FOR THE TEAM LEADER ..... 7

H. RECORDS RETENTION..... 8

I. RESTRICTIONS ON USE ..... 9

J. STORAGE OF BODY-WORN CAMERA RECORDINGS..... 9

K. BODY-WORN CAMERA RECORDINGS ..... 9

L. TRAINING ..... 11

M. THE ROLE OF THE PROGRAM MANAGER..... 12

A. PURPOSE

The purpose of this SOP document is to provide technical guidance to support USDA OIG's BWC program and Office of Investigations (OI) and Office of Compliance and Integrity (OCI) overall compliance with IG-8476, *Body-Worn Cameras*. As such, this guidance acts as a supplement to support OI and OCI Headquarters and field personnel to carry out their required duties as per IG-8476.

B. INTRODUCTION

Directive IG-8476 defines the specific roles and responsibilities pertaining to the management and use of BWCs and the digital evidence generated. This SOP serves as a technical guide, organized by role and activity. It is important to note that roles are not mutually exclusive, and one person can serve more than one role at one time. For example, the Team Leader has unique responsibilities, but is also responsible for all duties pertaining to the recording OIG employee.

Anyone with questions or comments regarding the content of this SOP should contact OIG's BWC Program Manager (PM).

C. GUIDANCE FOR OIG Criminal Investigators

Through the use of BWCs, OIG recognizes that transparency and accountability in law enforcement operations build trust with the communities we serve. As per IG-8476, all OIG Criminal Investigators will be assigned OIG-issued digital BWCs and are responsible for the proper charging, operation, and uploading of camera footage as described therein. OIG Criminal Investigators are also responsible for understanding their duties by completing all required training regarding BWCs. The following outlines technical guidance to support OI and OCI compliance with IG-8476 prior, during, and after an enforcement operation. For answers to frequently asked questions, please see Attachment A.

D. DEPLOYMENT OF BWCs FOR ENFORCEMENT OPERATIONS

The pre-operational briefing shall include a discussion of any steps that can be taken to avoid recording undercover personnel or confidential human sources (CHS).

1. USDA OIG-Led Enforcement Operations. When conducting a USDA OIG-led enforcement operation with a partner law enforcement agency, the Team Leader shall have a discussion, prior to the initiation of the law enforcement operation, with the partner agency's team leader and/or team members. Such discussions will include BWC deployment during the joint operation. The discussions shall include briefing the partner agency on the OIG BWC policy and reviewing the partner agency's BWC policy, if applicable. All practicable effort should be taken to resolve any concerns related to undercover agents. The lead OIG Criminal Investigator will memorialize these discussions in the OIG Enforcement Operational Plan.

2. Other Agency-Led Enforcement Operations. When USDA OIG is not the lead on a law enforcement operation involving a partner law enforcement agency, the Team Leader will brief, prior to the initiation of the law enforcement operation, the partner agency's team leader and/or team members concerning the OIG BWC policy. All practicable effort should be taken to resolve any concerns related to undercover agents involved with the enforcement operation. The lead OIG Criminal Investigator will memorialize these discussions in the OIG Enforcement Operational Plan, or in situations where the other agency is drafting the Enforcement Operational Plan, and not USDA OIG, these discussions should be documented in a separate Memorandum of Activity (MOA) to the file. The Special Agent in Charge (SAC), or as applicable the Director of OCI, with oversight responsibility of the operation shall be notified immediately of any unresolved conflicts with any partner agency related to BWC deployment. If the SAC, or as applicable the Director of OCI, is unable to resolve the conflicts, the Assistant Inspector General for Investigations (AIG/I), or as applicable the Deputy Inspector General (DIG), or their designee, should be notified immediately.
3. BWC Activation: The Team Leader shall give the command to initiate the recording of audio and video by all OIG Criminal Investigators to effectuate a law enforcement operation where BWCs are required. If, while wearing a BWC pursuant to this policy, an OIG Criminal Investigator encounters a subject who is uncooperative, violent, assaultive, or discussing criminal conduct that, in the applicable OIG employee's judgement, consistent with their training and experience, could lead to use of physical or deadly force, or be relevant to the investigation, the OIG Criminal Investigator should activate their BWC.
4. BWC Deactivation: BWCs shall be deactivated by OIG Criminal Investigators only upon the direction of the Team Leader when determined, at the Leader's discretion, the scene is secured. For purposes of this policy, the term "secured" means that the scene is safe and under law enforcement control.
  - a. Planned Arrests: When executing an arrest warrant or arresting an individual during the execution of a search warrant, the Team Leader may authorize the deactivation of specified BWCs once they have determined they are no longer required because the scene is secure and any arrestees are handcuffed, searched, and placed in the transport vehicle(s). While on the scene of an arrest, and during prisoner transports from the scene of an arrest, OIG Criminal Investigators must continue to wear their BWCs and leave them in the ready (i.e., buffering for that 2 minute maximum of the unit) or equivalent mode.
  - b. Search Warrants: When executing a search warrant, the Team Leader may authorize OIG Criminal Investigators to deactivate their BWCs once the location to be searched has been secured and all subjects have been searched and deemed not to be a potential threat. The Team Leader will use their

discretion to determine when team members conducting perimeter security during the execution of the warrant may deactivate their BWCs.

- c. Interviews: During the above-described law enforcement operations, a BWC may be used to record an interview with an arrestee or detainee in accordance with IG-8410 and I-15-004-8410.
- d. Deviations: Prior to the operation, policy deviations must be addressed in a decision memorandum from the Criminal Investigator to the AIG/I, or as applicable to the Director of OCI, through the SAC overseeing the operation. Under exigent circumstances, an oral authorization may be given by the AIG/I or their designee but must be subsequently documented.

5. Deviations from policy related to BWC activation, deactivation, or removal shall be addressed as follows:

- (1) Team Leader Approved: The Team Leader may authorize OIG Criminal Investigators to deactivate their BWCs if the law enforcement operation is of such a duration that BWCs need to be deactivated to conserve power and/or for temporary secure storage.
- (2) Employee Initiated: An OIG Criminal Investigator may deactivate independently their BWC at any time they need to obtain emergency medical attention or attend to a personal matter that takes them away from a planned operation, such as using the restroom.
- (3) Pre-Approved Deviations: Prior to an applicable law enforcement operation, policy deviations must be addressed in a decision memorandum from the Team Leader to the SAC through the Assistant Special Agent in Charge (ASAC), or as applicable the Director of OCI, overseeing the operation.
- (4) Unplanned Deviations: Any deviation from policy related to BWC activation or deactivation due to device malfunction, operator error, or other circumstances, shall be documented in the Additional Information section of IG-8473, Exhibit C (Enforcement Operational Plan) submitted by the Team Leader to the SAC (copy to the PM) through the ASAC, or as applicable the Director of OCI, overseeing the operation.

#### E. BODY-WORN CAMERA OPERATION

BWCs are sensitive to temperature. Do not store a BWC in a car or unnecessarily expose it to direct sunlight for extended periods of time. Avoid storing where sustained temperatures are at or greater than 95 degrees or at or less than -4 degrees Fahrenheit.

OIG Criminal Investigators should ensure that their assigned BWC is fully charged

before its deployment. No OIG Criminal Investigator shall be allowed to participate in a role requiring BWC use during a law enforcement operation if they do not have a fully charged and operational BWC. OIG Criminal Investigators will notify the BWC PM of any equipment malfunctions as soon as possible.

BWCs shall be set to buffer 2 minutes of video only, which will be included as part of the overall digital video footage. The BWC is technically incapable of capturing audio during the buffering period.

1. Prior to an enforcement operation:

- a. Fully charge the BWC (check “status bar” icon to ensure it is fully charged);
- b. Power up the BWC (a blinking green light indicates the camera is on);
- c. Activate the BWC at the command of the Team Leader. A blinking red light indicates the camera is recording.;
- d. Ensure “mute mode” is not activated (the microphone graphic will have a slash through it); and
- e. Disable sound and haptic (i.e., tactile) alerts for safety purposes (Press and continually hold the down-volume button for 3 seconds).

2. During an enforcement operation, activate and/or deactivate the BWC in accordance with IG-8476.

3. After an enforcement operation:

- a. As soon as possible and within 72 hours of use, upload video by inserting the BWC into the camera dock; and
- b. Ensure video footage was received intact at the designated software-as-a-service repository.

F. PLACEMENT OF THE BWC

1. If a tactical ballistic vest is worn, the BWC will be worn on the outside/front of the tactical ballistic vest. The tactical ballistic vest will be worn over the OIG Criminal Investigator’s clothing.
2. In the event a BWC is deployed when a tactical ballistic vest is not worn, the BWC will be secured to the OIG Criminal Investigator’s outer clothing, at or in the chest area.

3. When possible, OIG Criminal Investigators shall ensure the BWC is not obstructed by clothing or other objects on the OIG Criminal Investigator's person. OIG Criminal Investigators should not alter tactically-sound principles to accommodate the BWC's visual recording. OIG Criminal Investigators shall seek cover and concealment and use proper tactics to ensure their safety while wearing the BWC even if doing so obstructs the BWC's field of view coverage.
4. If an undercover Criminal Investigator or Confidential Human Source (CHS) participates in a law enforcement operation and the OIG Criminal Investigators on the scene have reason to believe they may have recorded the identity of the undercover Criminal Investigator or CHS, the Team Leader will inform the BWC PM without delay, and note this occurrence in the MOA memorializing the operation. The BWC PM will coordinate with the prevailing legal authority (OC; DOJ; State; or local prosecutors, as applicable) on what steps should be taken to address (i.e., redact, obscure, alter, or otherwise conceal) any images and voice recordings of any undercover personnel or CHS, if needed.
5. In situations where sensitive law enforcement information or high confidentiality impact level information is recorded with the BWCs, and the information cannot be adequately protected through the use of redaction methods, such as undercover personnel or CHS, the BWC PM will generate a hash value for the recording, save a copy to the storage location, protect it at a high impact level, designate it for sensitive law enforcement information, verify the hash value match of the original digital recording file and the copy, and then purge the original recording from evidence after receiving approval from the relevant legal authority.

#### G. GUIDANCE FOR THE TEAM LEADER

Team Leaders are responsible for communicating expectations and ensuring the proper use of OIG BWCs during an enforcement operation. Team Leaders also serve as the liaison with partnering agencies regarding BWC policies and deployment of BWCs. The following outlines technical guidance to support Team Leaders' compliance with IG-8476 prior to, during, and after an enforcement operation. As Team Leaders are also Criminal Investigators, they must comply with all required duties for that role as well. Please see the "Guidance for the OIG Criminal Investigators" section in this SOP for details. For answers to frequently asked questions, please see Attachment A.

1. At least 10 business days before a planned law enforcement operation, or as soon as practicable, notify the BWC PM ([OIG-INV-BWC@oig.usda.gov](mailto:OIG-INV-BWC@oig.usda.gov)), of the planned operation and specify attending personnel assigned a BWC.

Note: As is the nature of law enforcement, unplanned operations can and will occur, as well as situations where the use of a BWC is necessary. In these cases, the Team Leader will notify the PM as soon as practicable, even if that notice occurs after the unplanned operation.

2. Prior to conducting a law enforcement operation:
  - a. Conduct a briefing for all participating OIG Criminal Investigators regarding the planned use of BWCs.
  - b. If operation is OIG-led, liaison with participating agencies per IG-8476 regarding the use of BWCs; identify undercover personnel or CHS who may be subject to being recorded.
  - c. If operation is led by another agency, liaison with the lead agency per IG-8476 regarding the use of BWCs; identify undercover personnel or CHS who may be subject to being recorded.
3. During a law enforcement operation, give the command to activate BWCs in accordance with IG-8476.
4. After a law enforcement operation:
  - a. Give the command to deactivate BWCs based on tactical considerations and in accordance with IG-8476.
  - b. Ensure all participants prioritize the upload of video footage upon cessation of the operation, in accordance with IG-8476.
  - c. Contact the PM to verify all BWC footage was successfully uploaded by all participants.
  - d. Document corrupted or missing video files via email to the PM.

#### H. RECORDS RETENTION

1. BWC digital recording files that are not associated with allegations or complaints made against OIG employees and do not contain information pertinent to the allegation or complaint being investigated (i.e., preliminarily or formally) will be deleted 10 years following Complaint or Investigation closure, unless a request to continue retention is provided in writing to the BWC PM through the AIG/I, or as applicable the Director of OCI, or their designee. These digital recording files will be maintained via an approved storage service, where they were uploaded initially.
2. Upon receipt of a litigation hold, the Program Manager shall retain all relevant records until such time as the litigation hold is released pursuant to a memorandum from OC. The Program Manager shall retain all documentation related to the litigation hold.



3. BWC digital recording files associated with information pertinent to the complaint or investigation being undertaken, such as a spontaneous statement of a subject, witness, or law enforcement officer, will be kept with the complaint or investigation file, in accordance with OIG's records retention policy and consistent with Federal law.
4. BWC digital recording files associated with use of force incidents involving OIG employees, complaints or allegations made against OIG employees, or any other investigation of OIG employees, will be retained as directed by the Director of OCI, or their designee, in consultation with the Deputy Inspector General (DIG) and Office of Counsel (OC).

#### I. RESTRICTIONS ON USE

1. **Prohibited Use of BWCs:** Absent approval from the AIG/I, or as applicable the Director of OCI, or their designee, and in consultation with prevailing legal authority, BWCs shall not be used to record: (a) in a detention facility, if the law enforcement operation is not taking place in the facility; or (b) personnel conducting activities involving classified information, as determined by the AIG/I, or as applicable the Director of OCI, or their designee.
2. **Redacting BWC Recordings:** In any situation where BWCs record content that otherwise should not be shared because of the above section I.1 restrictions, or any other law enforcement sensitivities or privacy concerns, which could include recordings of undercover personnel, CHS, sensitive investigative techniques or equipment, minors, injured or incapacitated individuals, or sensitive locations such as restrooms, locker rooms, or medical facilities, the BWC PM, in consultation with the AIG/I, or as applicable the Director of OCI, or their designee, and the prevailing legal authority may address (i.e., redact, obscure, alter, or otherwise conceal), as authorized, any images and voice recordings of such concern when making copies of BWC recordings for disclosure.

#### J. STORAGE OF BODY-WORN CAMERA RECORDINGS

BWC footage will be controlled by the BWC PM. Each digital recording file will contain all relevant metadata, such as the date and time of the recording, the name of the OIG employee who recorded it, and, whenever possible, the investigation title and file number. An audit log will automatically be created and maintained that sets forth the history of each digital recording file, the date and time each digital recording file is reviewed, the purpose of each review and the name of each reviewer.

#### K. BODY-WORN CAMERA RECORDINGS

1. **Requests for Disclosure of BWC Recordings:** All requests for disclosure of BWC recordings and/or related information shall be coordinated through the

BWC PM, in consultation with the OC and the AIG/I, or as applicable the Director of OCI, or their designee. All requests for disclosure of BWC recordings will be referred to OC for review and processing. If it is necessary to make any type of alteration to the BWC digital recording file, the prevailing legal authority will direct in writing the BWC PM to make such alterations which will be reviewed by OC prior to formal implementation then disclosure.

2. **Deleting Recordings:** Any request to delete a portion or portions of any BWC digital recording files (e.g., accidental recording occurred) must be submitted in writing, via a memorandum from the Team Lead, or recording generating OIG employee, through their ASAC and the SAC after consultation with OC and OIG's Records Officer to the AIG/I, or as applicable the Director of OCI, or their designee, for approval. The memorandum must denote the reason(s) for the requested deletion in or of the recording. If the request is approved, the approved request memorandum will be provided to the BWC PM. The BWC PM may apply the approved deletion in or of the recording only after receiving the AIG/I, or as applicable the Director of OCI approved requested memorandum. All requests and final decisions will be maintained by the BWC PM.
  
3. **Access and Review of BWC Recordings:** Access to stored BWC digital recording files will be password protected, logged automatically by the system software, and audited periodically by the BWC PM to ensure only authorized users access the recordings and associated data for official and authorized purposes. All logins, access to video, and other actions occurring in the system's software are memorialized automatically in an audit trail log that is reviewable by the BWC PM and the BWC PM's supervisor. This information may be discoverable and could be requested by the prosecution or the defense counsel during court proceedings.
  - a. **Permitted Reviews of BWC Digital Recording Files:**
    - (1) **Permitted Reviews:** Only the recording generating OIG employee may access their BWC digital recording files when necessary to perform their official duties, including, but not limited to such review necessary to draft and review a Memorandum of Activity (MOA), Memorandum of Interview (MOI), Report of Investigation (ROI), or any other applicable documentation for the purposes of detailing aspects of a law enforcement operation.
  
    - (2) **Criminal Investigator-Involved Shootings/Uses of Force:** All Criminal Investigator-Involved shootings (CIIS) or other use of force incidents (including deadly force) should be handled in accordance with OIG's Use of Force policy and procedures (IG-

8472 and IG-8472-P). Additionally, the involved Criminal Investigator(s) and any other OIG employee(s) who witnessed the CIIS or use of force should provide their BWCs to the on-scene supervisor or Team Leader. If the on-scene supervisor is involved or witnessed the CIIS or use of force, the BWCs should be provided to the next senior Criminal Investigator on-scene. The on-scene supervisor or other senior Criminal Investigator should upload the videos from all the BWCs collected in accordance with Storage of BWC Recordings. The involved Criminal Investigator(s) and any other OIG employee(s) who witnessed the CIIS or use of force shall not be permitted to view their BWC recording without the concurrence of the prevailing legal authority.

- (3) Internal Investigations: OIG personnel conducting internal investigations may review BWC recordings in connection with such investigations. Requests to review an OIG employee's BWC recordings for the purpose of this subsection shall be made in a memorandum to the AIG/I and/or Director of OCI. The memorandum shall state the reason(s) for the request.
- (4) Training: BWC digital recording files from OIG law enforcement operations may not be used for training purposes.
- (5) Supervisors may not use BWC recordings as evidence to support a negative performance appraisal. However, supervisors may view BWC recordings to conduct "after action debriefs" and for acquiring information to then be passed for training purposes, as described above. Requests to review an OIG employee's BWC recordings for the purpose of this subsection shall be made in a memorandum to the SAC, or as applicable the Director of OCI. The memorandum shall state the reason(s) for the request.

## L. TRAINING

Training for BWC deployment consists of three parts:

1. Prior to deployment of BWCs, each OIG Criminal Investigator must complete a USDA OIG-*approved* initial training module to ensure the proper use and operation of the BWC, as well as compliance with privacy and civil liberties laws.
2. OIG Criminal Investigators must complete a semi-annual BWC familiarization module in AgLearn in conjunction with control tactics training or firearms training, to maintain proficiency in the use of BWCs and ensure continued proper functionality of the devices. If OIG employees are unable to complete the required

scheduled training, they will raise the need for alternate training with their ASAC, or as applicable the Director of OCI. The ASAC, or as applicable the Director of OCI, in conjunction with the PM, shall review and approve their alternate training.

OIG Criminal Investigators must receive a refresher module in AgLearn during annual in-service training to ensure the proper use of the BWC, as well as compliance with privacy and civil liberties laws. In addition to the required training modules, OIG Criminal Investigators may be asked to activate their BWCs during the course of normal training exercises for the purposes of routinely testing the equipment and simulating real-world scenarios that may arise regarding the operation of BWCs during a law enforcement operation. As part of the exercise, OIG employees shall upload any recorded training footage.

#### M. THE ROLE OF THE PROGRAM MANAGER

As described in IG-8476, the BWC PM will be an individual appointed by the AIG/I, or their designee, and is responsible for the overall management of the BWC program. Among other duties as described in IG-8476, the PM establishes the following roles and assigns appropriate permissions:

1. Identifies Program Administrators;
2. Configures Groups;
3. Configures Evidence Groups;
4. Configures custom Roles and Permissions;
5. Configures account settings;
  - a. Configures and adds users
  - b. Confirms and adjusts device settings, as needed
    - (1) 2-minute buffer
  - c. Configures Categories and Retention Policies
  - d. Configures Evidence ID validation
  - e. Enables IP address security
6. Deactivates users who have left the agency or no longer have a need to access video files;
7. Confirms with each Team Lead that an Operational Group was created, and users added;
8. When appropriate, assigns video as restricted or confidential; and
9. Adds users and/or groups who require access, e.g., supervisors.

**Attachment A. Frequently Asked Questions (FAQ)**

Q: *What is the maximum number of hours my BWC can record?*

A: BWCs can collect approximately 4 hours of footage; however, the length of time BWCs can continue to record can be negatively affected by adverse conditions, such as extreme temperatures.

Q: *Can I use my BWC for interviews?*

A: Yes; however, use of this electronic recording device in this capacity requires adherence with IG-8410 and I-15-004-8410.

Q: *I am concerned that my BWC may start making unprompted sounds or vibrates during an operation. Can the Program Manager mute signals that emanate from my BWC, e.g., light, sound, and haptics (tactile responses)?*

A: Yes, but you can mute them as well by holding the volume-down button down for 3 seconds. This is not to be mistaken for the ability to mute recording of audio, which is not authorized.

Q: *Will I be able to pair my BWC to my phone?*

A: Undecided at this time. INV is currently exploring this capability via Axon View.

Q: *Will Axon's Signal Sidearm force us all to acquire a SafariLand or Blackhawk holster?*

A: No. There is an adhesive option for "other" holsters if Criminal Investigators prefer to use their existing one.

Q: *Will I have access to transcription features?*

A: Yes, an available option to be leveraged when required, (i.e., a request from legal authority) is available through the BWC contract company.

Q: *Is my BWC going to be wireless capable?*

A: Yes, INV has activated LTE wireless for all BWCs.

Q: *What happens if there is an interruption of service during upload?*

A: The upload resumes upon reconnect.

Q: *What happens once the BWC video is uploaded?*

A: The video on the camera is deleted automatically.