



## Body Worn Cameras

| <u>Section</u>   | <u>Page</u>        |
|--|--------------------|
| <a href="#">Section 1. Overview</a>  | <a href="#">2</a>  |
| <a href="#">Section 2. Joint Operations</a>                                  | <a href="#">2</a>  |
| <a href="#">Section 3. Pre-Operational Planning and Briefing</a>             | <a href="#">2</a>  |
| <a href="#">Section 4. Deployment of BWCs for Enforcement Operations</a>     | <a href="#">3</a>  |
| <a href="#">Section 5. Deviation from BWC Policy</a>                         | <a href="#">4</a>  |
| <a href="#">Section 6. Placement of BWCs</a>                                 | <a href="#">4</a>  |
| <a href="#">Section 7. Deployment in Other Instances</a>                     | <a href="#">5</a>  |
| <a href="#">Section 8. Storage of BWC Recordings</a>                         | <a href="#">5</a>  |
| <a href="#">Section 9. Records Retention</a>                                 | <a href="#">5</a>  |
| <a href="#">Section 10. Restrictions on Use</a>                              | <a href="#">6</a>  |
| <a href="#">Section 11. BWC Equipment</a>                                    | <a href="#">7</a>  |
| <a href="#">Section 12. BWC Recordings</a>                                   | <a href="#">7</a>  |
| <a href="#">Section 13. Treatment of BWC Recordings and Release Requests</a> | <a href="#">9</a>  |
| <a href="#">Section 14. Training</a>   | <a href="#">10</a> |
| <a href="#">Section 15. References</a>                                       | <a href="#">10</a> |

**NOTE:** This policy will take effect upon the purchase of body worn camera equipment and the full implementation of the Defense Criminal Investigative Service body worn camera program and after any pilot and training programs have occurred.

**Section 1. Overview**

- 1-1 This instruction establishes Defense Criminal Investigative Service (DCIS) policy and procedures, required by Executive Order 14074, “Advancing Effective Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety,” May 25, 2022, on a DCIS Body Worn Camera (BWC) program.
- 1-2 BWC equipment shall only be used in conjunction with official law enforcement and investigative activities involving members of the public. The safety of DCIS personnel and members of the public are the highest priorities. A Special Agent (SA) who fails to activate a BWC because an incident unfolds too quickly making activation impracticable or unsafe does not violate this policy. Approved exceptions are outlined in Section 4-7 of this policy.

**Section 2. Joint Operations**

- 2-1 When conducting enforcement operations with a partner law enforcement agency that will deploy BWCs during the operation, DCIS SAs will comply with this Instruction. This section applies to both DCIS-led enforcement operations and other agency-led enforcement operations.
- 2-2 Prior to an operation using BWCs, the Special Agent in Charge (SAC) overseeing the operation shall notify the Assistant Inspector General for Investigations, Investigative Operations Directorate (AIGI-OPS) or their designee of any unresolved conflicts with any partner law enforcement agency regarding BWC deployment during the operation.
- 2-3 Any deviation from the DCIS BWC policy must be approved, in writing, by the AIGI-OPS, or their designee, and documented in the Operational Plan. Prior to the operation, policy deviations must be addressed in a decision memorandum from the DCIS case agent to the AIGI-OPS through the SAC overseeing the operation. Under exigent circumstances, an oral authorization may be given by the AIGI-OPS, or their designee, but must be subsequently documented.

**Section 3. Pre-Operational Planning and Briefing**

- 3-1 Prior to conducting an enforcement operation, the Resident Agent in Charge (RAC) or their designee will discuss the planned use of BWCs during the operational briefing. The briefing shall include a discussion of any steps that can be taken to avoid recording undercover agent (UCA) personnel or Confidential Human Sources. All DCIS SAs who are issued BWCs and who are expected to activate them during an operation must receive the operational briefing.
- 3-2 Prior to the execution of a search warrant or arrest warrant, the DCIS RAC, or their designee, will also brief all members of the search or arrest team.

- 3-3 **DCIS-Led Enforcement Operations.** When conducting a DCIS-led enforcement operation with a partner law enforcement agency, the RAC will discuss BWC deployment during the joint operation with the partner agency's team leader and/or team members, prior to the enforcement operation. The discussions shall include briefing the partner agency on the DCIS BWC policy and reviewing the partner agency's BWC policy, if applicable. Special care should be taken to resolve any issues related to UCAs. The DCIS case agent will document these discussions in the Operational Plan.
- 3-4 **Other Agency-Led Enforcement Operations.** When DCIS is not the lead on an enforcement operation with a partner law enforcement agency, the DCIS RAC will brief the partner agency's team leader and/or team members of the DCIS BWC policy, prior to the enforcement operation. Special care should be taken to resolve any issues related to UCAs involved with the enforcement operation. The DCIS case agent will document these discussions in the Operational Plan or in cases where the other agency is drafting the Operational Plan, and not DCIS, these discussions should be documented in a separate Investigative Activity Report (IAR).
- 3-5 The SAC overseeing the operation shall be notified immediately of any unresolved conflicts with any partner agency related to BWC deployment. If the SAC is unable to resolve the conflicts, the AIGI-OPS or their designee should be notified immediately.

#### **Section 4. Deployment of BWCs for Enforcement Operations**

- 4-1 DCIS SAs will wear and activate DCIS-issued BWCs for the purposes of recording their actions during the tactical portion of enforcement operations where the use of force may reasonably be anticipated, such as the planned execution of a search warrant or arrest.
- 4-2 **BWC Activation.** Upon the direction of the On-Site Team Leader, RAC, or their designee, all participating DCIS SAs upon approaching a subject or premises during an enforcement operation shall activate BWCs. The On-Site Team Leader, RAC, or their designee, can direct an agent to re-engage BWC recording at any time during an enforcement operation.
- 4-3 **BWC Deactivation.** BWCs shall be deactivated by DCIS SAs only upon the direction of the RAC, or their designee, when the supervisor determines, at their discretion, the scene is secured. For purposes of this policy, the term "secured" means that the scene is safe and under law enforcement control.
- 4-4 **Search Warrants.** When executing a search warrant, the On-Site Team Leader, RAC or the RACs designee, may authorize DCIS SAs to deactivate their BWCs once the location to be searched has been secured and all subjects have been searched. The On-Site Team Leader, RAC, or their designee, will use their discretion to determine when team members conducting perimeter security during the execution of the warrant may stop recording.

- 4-5 **Planned Arrests.** When executing an arrest warrant or arresting an individual during the execution of a search warrant, the RAC, or their designee, may authorize the deactivation of most BWCs once he or she has determined the scene is secure and any arrestees are handcuffed and placed in the transport vehicle. At least one law enforcement officer shall stay with each arrestee to ensure safety and to monitor the arrestee's health. While on the scene of an arrest and during prisoner transports from the scene of an arrest, DCIS SAs must continue to wear their BWCs and leave them in the Ready (Buffering) or equivalent mode should a use of force incident occur.
- 4-6 **Exceptions to BWC Activation.**
- The On-Site Team Leader, the RAC, or their designee, may authorize DCIS SAs to deactivate their BWCs if the enforcement operation is of such a duration that BWCs need to be deactivated to conserve power and/or for temporary storage.
  - A DCIS SA may deactivate their BWC at any time the SA needs to obtain emergency medical attention or needs to attend to a personal matter that takes him or her away from a planned operation, such as using the restroom.

### **Section 5. Deviation from BWC Policy**

- 5-1 Deviations from policy related to BWC activation or deactivation shall be handled as follows.
- 5-2 **Pre-Approved Deviations.** The AIGI-OPS, or their designee, with an Office of General Counsel legal sufficiency review, must approve, in writing, any deviation from the DCIS BWC policy and if applicable, the DCIS SA must document the deviation in the Operational Plan. Prior to the operation, policy deviations must be addressed in a decision memorandum from the DCIS case agent to the AIGI-OPS through the SAC overseeing the operation. See Attachment A for a Sample Decision Memorandum.
- 5-3 **Unplanned Deviations.** Any deviation from policy related to BWC activation or deactivation due to device malfunction, operator error, or other circumstances, shall be documented, within 48 hours, in a memorandum from the DCIS case agent to the SAC overseeing the operation through the RAC and a copy must be provided to the BWC Program Manager (PM). The DCIS SA must upload a copy of the unplanned deviation to the applicable Case Reporting and Information Management System (CRIMS) Virtual Case File (VCF). The memorandum shall address: (1) why the recording was not made; (2) why the recording was interrupted; and/or (3) why the recording was terminated.

### **Section 6. Placement of BWCs**

- 6-1 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 DCIS SA's clothing.
- 6-2 In the event a BWC is deployed when a tactical ballistic vest is not worn, the BWC will

be secured to the DCIS SA's outer clothing.

- 6-3 DCIS SAs should ensure the BWC is not obstructed by clothing or other objects on the SA's person and is capturing what is in front of the SA. DCIS SAs should not alter tactically-sound principles to accommodate the BWC's visual recording. DCIS SAs should remember to seek cover and concealment and use proper tactics to ensure their safety while wearing the BWC even if doing so obstructs the BWC's coverage.
- 6-4 If an undercover agent participates in the operation and the DCIS SAs on the scene are not able to take measures to avoid recording the identity of the undercover agent, the RAC will inform the BWC PM and note this occurrence in the IAR memorializing the operation. The BWC PM will coordinate with the Office of General Counsel on what steps should be taken to redact any images and voice recordings of any undercover agents.

### **Section 7. Deployment in Other Instances**

- 7-1 The deployment of BWCs is not intended to supersede existing DCIS policy regarding interviews or other evidence collection.

### **Section 8. Storage of BWC Recordings**

- 8-1 BWC recordings will be uploaded as soon as possible, usually within 24 hours, and stored in a DCIS-controlled cloud storage service, with any vendor access logged. Access to the recordings will be controlled by the BWC PM. Each file will contain all relevant metadata, such as the date and time of the recording, the name of the DCIS SA who recorded it, and whenever possible the case name and number. An audit log will automatically be created and maintained that sets forth the history of each recording, the date and time each recording is reviewed, and the name of each reviewer.

### **Section 9. Records Retention**

- 9-1 BWC recordings will be securely stored according to DCIS-mandated retention procedures as outlined in DCIS Special Agents Manual (SAM) Chapter 42, Investigative Records Management.
- 9-2 BWC recordings that are not associated with complaints or allegations made against DCIS employees and do not contain information pertinent to the case being investigated will be maintained in accordance with DCIS SAM Chapter 42 unless a request is provided in writing to the BWC PM through the AIGI-OPS or their designee. These recordings will be maintained in a DCIS-controlled cloud storage service where they are initially uploaded.
- 9-3 BWC recordings associated with information pertinent to the case being investigated, such as spontaneous statement of a subject, witness, or law enforcement officer, will be kept with the case file in accordance with DCIS SAM Chapter 42, case records retention

policy, and consistent with federal law.

- 9-4 BWC recordings associated with use of force incidents involving DCIS employees, complaints or allegations made against DCIS employees, or any other investigations of DCIS employees, will be retained as directed by the AIGI-OPS, or their designee, in consultation with the Office of General Counsel. All use of force incidents where video footage is recorded will be reviewed in accordance with DCIS SAM Chapter 38, Use of Force.
- 9-5 BWC recordings associated with normal training exercises (i.e., no injuries) will be deleted after the appropriate instructor (Use of Force PM, firearms instructor, control tactics instructor, use of force instructor, etc.) reviews the recordings for teachable scenarios and confirms it is acceptable to delete the recording. If a teachable scenario is found, the instructor will ask the DCIS SA(s) involved if they would like their faces redacted and/or voices changed from the recording before the footage is used in future trainings. The BWC PM will redact faces and change voices, as requested. The unredacted BWC recording will be deleted after all changes are made to the training video.
- 9-6 In situations where sensitive law enforcement information or high confidentiality impact level information is recorded with the BWCs, such as undercover personnel or confidential human sources, the BWC PM will generate a hash value for the recording, save a copy to a separate DCIS-controlled storage location protected at a high impact level and designated for sensitive law enforcement information, verify the hash value match of the original recording and the copy, and then purge the original recording from the cloud storage system after receiving approval from the cognizant U.S. Attorney's Office, Department of Justice Division, or the Judge Advocate General Corps and the Office of General Counsel.

### **Section 10. Restrictions on Use**

- 10-1 DCIS SAs equipped with BWCs should be mindful of locations where recording may be considered insensitive, inappropriate, or prohibited by privacy policies. BWCs shall only be used in conjunction with official law enforcement duties and not personal activities.
- 10-2 **Prohibited Use of BWCs.** Absent approval from the AIGI-OPS, or their designee, in consultation with any assigned prosecutor or the Office of General Counsel if no prosecutor is assigned, BWCs shall not be used to record: (1) in a detention facility, if the law enforcement operation is not taking place in the facility or (2) personnel conducting activities involving classified information.
- 10-3 **Redacting BWC Recordings.** In any situation where BWCs record content that otherwise should not be shared because of the above restrictions or any other law enforcement sensitivities or privacy concerns, which could include recordings of undercover personnel, confidential sources, 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 Office of General Counsel, may use redaction software to blur images or portions of images, or minimize audio content, when making copies of BWC recordings for disclosure.

- 10-4 BWC use is limited to enforcement or investigative activities involving members of the public. The BWC recordings will capture video and audio evidence for use in criminal investigations, administrative reviews, and other proceedings protected by confidentiality laws and Department policy. Department members shall comply with all applicable laws and DCIS Instructions regarding confidential information. Unauthorized use or release of BWC recordings may compromise ongoing criminal and administrative investigations or violate the privacy rights of those recorded. Any unauthorized use or release of BWC recordings in violation of confidentiality laws and/or DCIS Instructions is prohibited. Any DCIS employee aware of unauthorized use or release of BWC recordings must disclose this information to their immediate supervisor, the DoD Office of Inspector General (OIG) Office of Professional Responsibility (OPR) and the DoD OIG Office of Security (OSEC).
- 10-5 Any DCIS employee aware of any BWC use inconsistent with this policy must disclose that information to their immediate supervisor, the DoD OIG OPR, and the DoD OIG OSEC.

### **Section 11. BWC Equipment**

- 11-1 DCIS SAs shall only use BWCs issued by DCIS. DCIS SAs should exercise reasonable care when using BWCs to ensure their proper functioning. DCIS SAs should ensure that the BWC is fully charged before and during its deployment.
- 11-2 **Storage.** DCIS SAs will not leave BWCs or any associated equipment stored in a government owned vehicle (GOV) at any time, including while TDY.
- 11-3 **Loss or Theft of Equipment.** DCIS SAs will report the loss or theft of a BWC to their immediate supervisor as soon as possible, but no later than 24 hours after the discovery of the loss or theft. The immediate supervisor shall notify the BWC PM and the Field Office SAC.
- 11-4 **Damaged, Malfunctioning, or Inoperable Equipment.** If a DCIS SA's BWC malfunctions or is damaged, the SA shall notify their RAC. The RAC will follow DoD OIG Policy outlined in Inspector General Instruction 7000.14, Volume 2, if the BWC is damaged.

### **Section 12. BWC Recordings**

- 12-1 The BWC equipment and all data, images, video, audio, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of DCIS. Other than the BWC PM or the BWC PM's supervisor, no DCIS personnel shall, edit, alter, erase,

duplicate, copy, share, or otherwise release, disclose, or distribute in any manner, any BWC recordings, without prior written authorization from the AIGI-OPS, or their designee, in consultation with the Office of General Counsel. DCIS SAs may review their own BWC recordings, subject to the restrictions below, but may not share their recordings with others.

- 12-2 **Deleting Recordings.** Any request to delete a portion or portions of the recordings (e.g., accidental recording) must be approved by the DCIS SA's prosecutor. Once approved the DCIS SA must submit a memorandum through their supervisor and the SAC, and obtain approval in writing from the AIGI-OPS, or their designee, in consultation with the Office of General Counsel. The memorandum must state the reason(s) for the request to delete the recording. If the request is approved, the request memorandum and the written approval will be provided to the BWC PM. The BWC PM may delete the recording only after receiving the requested memorandum and written approval.
- 12-3 All requests and final decisions will be maintained by the BWC PM.
- 12-4 **Access and Review of BWC Recordings.** Access to stored BWC recordings will be password protected, recorded automatically by the system software, and audited periodically by the BWC PM to ensure that only authorized users' access the recordings and associated data for legitimate and authorized purposes. All logins, video access, and other actions taken in the system software is placed 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 during court proceedings. In addition, this information may be requested as part of a DCIS internal management review or a DoD OIG OPR inquiry.
- 12-5 Permitted Reviews of BWC Recordings.
1. **Permitted Reviews.** A DCIS SA may access BWC recordings when necessary to perform the essential functions of their job, including but not limited to such review necessary to draft and review an IAR describing an operation. A DCIS SA may also access BWC recordings when necessary to respond to allegations of administrative or criminal misconduct or poor performance relating to the recorded enforcement activity, subject to the limitations of subsections (2) and (3) immediately below.
  2. **Reviews by Subjects.** A DCIS SA who is the subject of an administrative investigation relating to the recorded enforcement activity may review their own BWC recording prior to being interviewed by any DCIS or non-DCIS personnel investigating allegations about the DCIS SA's conduct. The DCIS SA may review their BWC recording with their attorney or other representative, provided the attorney or representative signs a non-disclosure agreement. The DCIS SA will not be permitted to make or take a copy of the recording.
  3. **DCIS Special Agent-Involved Shootings/Use of Force Incidents.** All DCIS SA-involved shootings (AIS) or other use of force incidents (including deadly force) should



be treated as being under criminal investigation unless and until the applicable federal, state, or local prosecution office(s) has declined prosecution. As soon as practicable and safe, after any such incident, the involved DCIS SA should be informed by their supervisor that they should not discuss the incident with anyone during the pendency of any preliminary investigation other than a personal or agency attorney. See DCIS SAM Chapter 38 for additional information on use of force incidents. The involved DCIS SA(s) and any other DCIS SA(s) who witnessed the AIS or use of force incident should provide their BWCs to the RAC. If the RAC is involved or witnessed the AIS or use of force incident, the BWCs should be provided to the Field Office Assistant Special Agent in Charge (ASAC) or their on-site designee. The RAC or other senior DCIS SA should upload the videos from all of the BWCs collected. The involved DCIS SA(s) and any other DCIS SA(s) who witnessed the AIS or use of force incident shall not be permitted to view their BWC recording without the concurrence of the assigned prosecutor.

4. **Internal Investigations.** DCIS personnel conducting internal investigations may review BWC recordings in connection with such investigations. Requests to review a DCIS SA's BWC recordings for the purpose of this subsection shall be made in a memorandum to the Inspections and Compliance PM. The memorandum shall state the reason for the request.
5. **Training.** The DCIS Training Division may approve the use of BWC recordings for training purposes. Access to those recording will be coordinated through the BWC PM. When necessary, the BWC PM, in consultation with the Office of General Counsel, will obtain the written permission of any DCIS personnel who recordings or images are depicted in any training videos.

### **Section 13. Treatment of BWC Recordings and Release Requests**

- 13-1 In all circumstances, BWC recordings shall be treated as law enforcement sensitive and controlled unclassified information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings. BWC recordings will also be treated as potential evidence in a federal investigation subject to applicable federal laws, rules, and policies concerning any such disclosure; and therefore, deemed privileged absent appropriate redaction prior to disclosure. All requests for DCIS BWC recordings unrelated to a pending DCIS criminal investigation or case will be forwarded to the BWC PM, who will consult with the Office of General Counsel, and determine whether recordings will be released. Nothing in this policy shall be deemed to provide a right of public access to BWC recordings. DCIS BWC recordings are controlled by, and the property of, the DCIS and will be retained and managed by the DCIS.
- 13-2 **Requests for Disclosure of BWC Recordings.** All official government requests for disclosure of BWC will be processed by the BWC PM, who will consult with the Office of General Counsel. Any routine Freedom of Information Act (FOIA) requests will be released pursuant to routine DoD OIG and/or DCIS policy.

**Section 14. Training**

- 14-1 The DCIS Training Division shall ensure that all DCIS SAs receive the required training on the use of BWCs in accordance with the policies in this chapter.
- 14-2 To ensure the proper use and operation of BWCs, as well as maintain compliance with privacy and civil liberties laws, DCIS SAs must establish and maintain proficiency and knowledge related to BWC deployment. Training for BWC deployment consists of three modules: (1) Initial, (2) Familiarization, and (3) Refresher.
- 14-3 Prior to deployment of BWCs, each DCIS SA must complete a DCIS-approved initial training module to ensure the proper use and operation of the BWC, as well as compliance with privacy and civil liberties laws.
- 14-4 DCIS SAs must complete a semi-annual BWC familiarization module in conjunction with control tactics training or firearms training, to maintain proficiency in the use of BWCs and ensure continued functionality of the devices. If DCIS SAs are unable to complete the required scheduled training, they will raise the need for alternate training with their RAC. The RAC shall review and approve their alternate training.
- 14-5 DCIS SAs must receive a refresher module during DCIS in-service training to ensure the proper use of the BWC, as well as compliance with privacy and civil liberties laws.

**Section 15. References**

- 15-1 These policies and procedures are in accordance with the following references:
- Deputy Attorney General Memorandum Regarding Body-Worn Camera Policy, June 7, 2021
  - Executive Order 14074, “Advancing Effective Accountable Policing and Criminal Justice Practices to Enhance Publics Trust and Public Safety,” May 25, 2022
  - DCIS Special Agents Manual Chapter 42, Investigative Records Management, August 2011
  - DCIS Special Agents Manual Chapter 38, Use of Force, October 2017

