

OIG Body-Worn Camera Policy

Summary: Establishes a policy framework for the use of body-worn cameras and the related digital evidence management system by FHFA-OIG employees.

Approval: Karl Kadon, Deputy Inspector General for Investigations

I. BACKGROUND

In response to Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, signed May 25, 2022, the following is the Federal Housing Finance Agency Office of Inspector General's (OIG) policy regarding body-worn cameras (BWCs). As mandated by Executive Order 14074, this policy is "designed to promote transparency and protect the privacy and civil rights of the public."

The use of BWCs by law enforcement fosters public trust, transparency, and accountability. BWCs enable law enforcement agencies to capture contacts with witnesses, subjects, targets, and the public during the enforcement actions, interviews, and other investigative activities.

While BWC recordings may enhance the Office of Investigation's (OI) ability to obtain evidence for investigative and prosecutorial purposes, it should be noted that the recordings may depict things that the Special Agent (SA) did not see or hear. Also, the SA may have heard or seen things that were not recorded by the BWC. While the BWC recordings depict visual and audio information from the scene, the human eye, ear, and brain are highly likely to perceive some things differently in stressful situations than how the camera records them.

In addition to BWCs, this policy also covers BWC-related applications and use of the digital evidence management system (DEMS) for BWC recordings. See the OIG Office of Investigations Policies and Procedures Manual (<u>OI Manual</u>) § 8.10 Digital Evidence Management System, for related policies and procedures applicable to BWCs and the DEMS.

All SAs are required to review the OIG Body-Worn Camera Policy annually.

II. **DEFINITIONS**

- A. Access Class: A designation in the DEMS used to control access to BWC recordings and other digital evidence within OIG. Axon Evidence uses three agency-defined access classes: Unrestricted, Restricted, and Confidential.
- B. Activation or Activate: Putting the BWC in Recording (Event) mode.

- C. **Axon Capture**: A smartphone application that records photographs, audio, and video. It syncs such recordings, including GPS location and metadata, to Axon Evidence.
- D. **Body-Worn Camera**: Overt mobile audio- and video-capture device issued to an SA to be used in accordance with this policy. OIG uses Axon BWCs.
- E. **Buffering or Pre-Event Buffering**: The duration of time the BWC preserves video recordings while in the "Ready" mode prior to activation of the BWC in the Recording (Event) mode. OIG has configured BWCs to preserve recorded video only (no audio) for 30 seconds prior to activating the BWC to Recording (Event) mode.
- F. **BWC (device) Audit Trail**: A chronological record showing events and changes for a BWC produced by the Axon Evidence digital evidence management system. The audit information can be filtered to a particular date range or show the entire life of the BWC.
- G. **BWC-DEMS Program Manager (Program Manager)**: An OIG employee assigned to serve as the BWC-DEMS System Administrator to support the BWC-DEMS Program.
- H. **BWC-DEMS System**: BWCs and all associated equipment, networks, software, and applications, and the DEMS.
- I. **BWC-DEMS System Administrator (System Administrator)**: An OIG employee who has been granted full access and data management rights for BWCs and the digital evidence management data system.
- J. **BWC Evidence**: BWC recordings of operational, enforcement, or investigative activities, including recordings made in the presence of a prisoner or detained person, including associated metadata and audit trails.
- K. **BWC Recordings**: For purposes of this policy, refers to audio and video recordings, and associated metadata from BWCs used by SAs.
- L. **Category**: A term used to identify the type of evidence or other item recorded by a BWC or other digital evidence stored in the DEMS, and which determines the length of retention and the access class attached to the item in the DEMS.
- M. **Digital Evidence**: Any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device.
- N. **Digital Evidence Management System**: A secure, centralized, cloud-based solution for storing, managing, investigating, and sharing digital evidence. OIG uses Axon Evidence (evidence.com) as the DEMS.
- O. **Evidence Action Request**: An automated request relating to unrestricted BWC evidence or other unrestricted digital evidence stored in the DEMS and relating to a case entered in the

Case Management System (CMS) submitted through the Evidence Tab in the official case file (OCF) in CMS.

- P. Evidence Audit Trail: A chronological record of all interactions with a piece of evidence automatically produced by the DEMS.
- Q. **Metadata**: Data in the BWCs and the DEMS that provides context or additional information about BWC recordings and other digital evidence stored in the DEMS.
- R. Ready (Buffering) Mode: Powering the BWC on and starting pre-event buffering.
- S. Recording (Event) Mode): While in this mode, the BWC will record both audio and video.
- T. **Removable Media**: Portable electronic storage devices, which can be inserted into and removed from a computing device, and used to store text, video, audio, and image information. Examples include hard disks, floppy disks, zip drives, CDs, DVDs, thumb drives, pen drives, and USB storage devices.
- U. **Secured**: For purposes of this policy, the term "secured," in reference to the execution of a search warrant or seizure order, means that the scene is safe and under law enforcement control as determined by the OIG supervisor on the scene, or by the senior OIG SA on the scene, if no supervisor is present.
- V. Serious Bodily Injury: The phrase "serious bodily injury" generally means an injury which is so severe as to require the hospitalization of those injured. NOTE: The term "serious bodily injury" is synonymous with the term "serious physical injury." See <u>OI Manual</u>, § 4.1 Critical Incident Response Use of Force.
- W. **Tag or Tagging**: A field in the DEMS that may be used to provide additional information or context about BWC recordings and other items stored in the DEMS.
- X. Use of Force Critical Incident: The term "critical incident" is defined as one in which there has been the use of force by a federal law enforcement officer in the line of duty that results in death or serious bodily injury. <u>OI Manual</u>, § 4.1.
- Y. User Audit Trail: A user audit trail shows many of the activities taken by the user in addition to changes to the user account.

III. ROLES AND RESPONSIBILITIES

A. The Deputy Inspector General for Investigations (DIGI) is responsible for implementation and oversight of OIG's BWC-DEMS Program. The DIGI may delegate duties, responsibilities, and authorities relating to the BWC-DEMS Program to the Assistant Inspector General, Investigations (AIGI), the Special Agent in Charge (SAC) for Headquarters Operations Region (SAC HQ OPS), and other senior OI employees.

- B. The SAC HQ OPS is responsible for day-to-day supervision of the BWC-DEMS Program.
- C. The Program Manager is responsible for the overall administration of the program and will report to SAC HQ OPS. Duties of the Program Manager include:
 - 1. Maintain or change configuration of the BWC-DEMS as directed by the DIGI or designee;
 - 2. Maintain files relating to the administration of the BWC-DEMS Program;
 - 3. Periodically review BWC recordings to evaluate the quality of the recorded video and audio to ensure that OIG SAs are properly operating BWCs and that the BWCs are functioning properly;
 - 4. Serve as Evidence Custodian for BWC evidence and other digital evidence items stored in the DEMS (see <u>OI Manual</u>, § 8.10 Digital Evidence Management System).
 - 5. Implement audit procedures for the BWC-DEMS Program as directed by the DIGI or designee;
 - 6. Assist OIG employees in using BWCs and the DEMS;
 - 7. Assist with redaction of BWC recordings;
 - 8. Provide training relating to the BWC-DEMS Program;
 - 9. Remain aware of significant issues affecting the use of BWCs and the DEMS including monitoring changes in technology and law, including maintaining close liaison with federal law enforcement partners; communicating with the BWC-DEMS vendor; reviewing relevant statutes, regulations, and caselaw; and attending training and conferences; and
 - 10. Such other duties as necessary to ensure the upkeep, configuration, and reliability of the BWC-DEMS System.
- D. BWC-DEMS System Administrators will generally assist as needed in the upkeep, configuration, and reliability of the BWC-DEMS System. They may also perform the duties of the Program Manager in the absence or unavailability of the Program Manager.
- E. SACs are responsible for ensuring that their subordinates use BWCs and the DEMS in compliance with applicable policies and procedures, and to review and audit use of the BWC-DEMS use as directed.
- F. The Information Technology Department will provide technical support to the BWC-DEMS Program.
- G. The Office of Counsel (OC) will provide legal support for the BWC-DEMS Program.

IV. DIRECTIONS FOR USE OF BODY-WORN CAMERAS AND ASSOCIATED APPLICATIONS

- A. OIG-issued BWCs, all associated equipment, applications, software, recordings, and other data are the sole property of FHFA-OIG. OIG personnel shall not use OIG-issued BWCs or any associated equipment, applications, and software for personal activities. Unauthorized use of BWCs or associated applications, or accessing, copying, or releasing recordings or other data, is prohibited and may result in disciplinary action.
- B. Use of privately owned BWCs is prohibited. SAs may possess and use only BWCs owned and issued by OIG while in an OIG facility or performing OIG duties. An SA will wear and use only one BWC at any one time.
- C. SAs must complete an agency-approved training program that includes proper use of BWCs and related applications, use of the DEMS, and applicable OIG policy. OIG will provide periodic training to ensure continued proficiency.
- D. SAs who have been issued BWCs and who have completed BWC-DEMS training as directed by OIG must use BWCs in accordance with this policy, other applicable OIG policies and procedures, and training.
- E. BWCs are assigned to individual SAs in the BWC-DEMS System. SAs are prohibited from using an unassigned BWC or one assigned to another SA.
- F. Other than limited user-preference settings such as volume or LED display, OIG personnel will not change BWC settings or functions, alter the operation of any BWC, or attempt to do so, unless designated as a System Administrator and specifically authorized by the DIGI or designee.
- G. OIG employees will not use any electronic device or any other means to intentionally interfere with or alter the capability or operation of a BWC or any other component of the BWC-DEMS System.
- H. OIG employees will not alter, tamper with, delete, damage, or destroy any BWC or BWC recording, or attempt to do so, unless specifically authorized.
- I. Only the Program Manager or other System Administrator is allowed to delete BWC recordings, and they may do so only in accordance with established OIG policies and procedures. See, e.g., <u>OI Manual</u>, § 8.10 Digital Evidence Management System.
- J. BWC recordings will not replace reports or other documentation required by OIG policies and procedures.
- K. OIG personnel will not copy BWC recordings, or post BWC recordings to the Internet, social media sites, or the media, or otherwise release or disseminate BWC recordings in any way, unless authorized to do so for an official OIG purpose.

- L. OIG employees should consult OC on legal questions pertaining to the use of BWCs and handling of BWC recordings.
- M. Access to stored BWC recordings and metadata is password-protected and recorded automatically by system software. The Program Manager, supervisors, and Headquarters management will periodically audit use of the BWC-DEMS System to ensure that only authorized users are accessing the data for authorized purposes. All logins, recording access, and other actions taken in the DEMS are noted in an audit trail log that is reviewable by the Program Manager, System Administrators, and Headquarters management.
- N. Metadata and other audit information may be discoverable and could be disclosed for use in criminal, civil, or administrative cases.

V. BODY-WORN CAMERA EQUIPMENT

- A. SAs must store BWCs in an OIG office or other secure location when not in use.
- B. SAs must safeguard BWCs containing BWC evidence and keep them secure in an OIG office, another secure location, or in their personal possession.
- C. The following applies to storage of BWCs containing evidence in unattended vehicles:
 - 1. SAs are prohibited from storing BWCs containing evidence in an unattended vehicle overnight.
 - 2. If necessary, SAs may store BWCs with evidence in an unattended vehicle only if the vehicle is equipped with an agency-approved hard-sided storage container that is securely anchored to the vehicle with a cable or chain that meets the requirements for firearms storage. The vehicle must be locked and the BWC secured in the locked storage container. SAs should minimize the amount of time BWCs with evidence are stored in vehicles and should refrain from parking on public streets, in public garages, or in public parking lots for long periods of time.

NOTE: Once evidence is uploaded to the DEMS it is automatically deleted from the BWC.

- D. SAs must report the loss, theft, or damage of a BWC to their immediate supervisor as soon as practical, but no later than 24 hours after the discovery of the loss, theft, or damage. The supervisor must then notify the Program Manager and the SAC HQ OPS as soon as practical.
- E. If the lost or stolen BWC contained BWC evidence, or if damage to a BWC may result in the loss of evidence, SAs must detail the circumstances in a Memorandum of Activity (MOA) within five working days and send it to the SAC HQ OPS, the Program Manager, and the assigned prosecutor. The case agent will add the MOA to the OCF.

VI. RECORDING WITH BODY-WORN CAMERAS AND RELATED APPLICATIONS

- A. Unless an exception stated in this policy applies, SAs must wear and activate their BWCs to record operational activities as set forth below. Unless otherwise stated, the BWC must be used to record both video and audio.
 - 1. Pre-Planned Arrests
 - a. SAs must wear and activate their BWCs to record a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, including the apprehension of fugitives sought on state and local warrants.
 - b. SAs must place their BWCs in the Ready (Buffering) mode prior to arrival at the scene of the arrest and activate them to Recording (Event) mode prior to approaching the person to be arrested or the location of the arrest.

Upon activation, SAs should state out loud, "*Body camera activated*," their name, location, the date, time, and time zone unless under the circumstances making a verbal statement is not safe or practical. In such cases, SAs may activate their BWCs and state this preamble at the pre-operation staging location.

c. SAs must continue to record until they leave the scene or until the subject is in custody and all law enforcement personnel have left the scene.

Prior to deactivating the BWCs, SAs should state "*Body camera deactivated*," their name, location, the date, time, and time zone.

- 2. Prisoner Transports
 - a. SAs must wear and record with their BWCs while transporting a prisoner from the scene of the arrest to the place of detention or until they turn the prisoner over to another custodial authority. The requirement to record prisoner transports applies only to the transport from the scene of the arrest to the initial place of detention or turnover to another custodial authority. It does not apply to later transports, e.g., extradition transports.

NOTE: SAs may stop recording to comply with a recording prohibition at the place of detention.

- b. Upon commencing a prisoner transport, SAs should verbally state, "*Body camera activated*," their name, location, destination for the prisoner transport, the date, time, and time zone unless under the circumstances making a verbal statement is not safe or practical.
- c. Prior to deactivating the BWC at the completion of a prisoner transport, SAs should state "*Body camera deactivated*," their name, location, the date, time, and time zone.

- 3. Search Warrants and Seizure Orders
 - a. SAs must wear and activate their BWCs to record the execution of a search warrant or seizure order.
 - b. SAs must place their BWCs in the Ready (Buffering) mode prior to arrival at the scene of the search warrant or seizure order and activate their BWCs to Recording (Event) mode prior to commencing execution of the search warrant or seizure order.

Upon activation, SAs should state out loud, "*Body camera activated*," their name, location, the date, time, and time zone unless under the circumstances making a verbal statement is not safe or practical. In such cases, SAs may activate their BWCs and state this preamble at the pre-operation staging location.

- c. Once the team leader or designated onsite supervisor determines the scene is secured, SAs assigned to conduct the search or seizure inside the premises must continue to wear their BWC and leave it in the Ready (Buffering) mode until the search or seizure is completed and they leave the scene unless they are directed by the onsite supervisor or team leader to start recording again.
 - i. If, during the execution of a warrant, the team leader or designated onsite supervisor determines that a particular activity should be recorded inside the premises, e.g., breaching a safe, the team leader or designated onsite supervisor will direct SAs to reactivate and record with their BWCs until that specific activity is completed.
 - ii. Upon commencing recording an activity inside the premises, SAs should state out loud, "*Body camera activated*," their name, location, the date, time, and time zone unless under the circumstances making a verbal statement is not safe or practical. Prior to deactivating the BWC at the completion of the activity, SAs should state "*Body camera deactivated*," their name, location, the date, time, and time zone.
- d. If an arrest is made during the execution of a search warrant or seizure order, SAs assigned to guard the prisoner must continue to record until the prisoner is transported from the scene. SAs assigned to transport the prisoner will record as set forth in § VI.A.2.
- e. Once the scene is secured, if any SAs are assigned to exterior cover/perimeter posts in public view while the search is conducted, they must continue to wear their BWCs and keep them powered on in the Ready/Buffering mode. The team leader or designated onsite supervisor may direct the exterior perimeter SAs to continue recording after the scene is secured until they leave or all law enforcement personnel leave the scene based on their assessment of the operational security and safety situation.

- f. Prior to deactivating the BWC, SAs should state "*Body camera deactivated*," their name, location, and the date, time, and time zone.
- g. The requirement to record with BWCs does **not** apply in the following circumstances:
 - i. Searches of physical property or a device already in government custody or control in a law enforcement or government facility (e.g., a vehicle, computer, or mobile phone already in OIG custody);
 - ii. Search warrants to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records;
 - iii. A lawfully authorized "sneak and peek" search warrant (also referred to as "delayed notice" or "covert entry" search warrant) where the intent is to surreptitiously enter an unoccupied premises and clandestinely search the premises in a manner to disguise law enforcement involvement; or
 - iv. A delayed notice search warrant or court order authorizing surreptitious entry onto a premises to install video and/or audio surveillance equipment.
- B. Unless an exception applies, BWC recording requirements apply to all OIG participants in the above activities regardless of whether it is a federal, state, or local case, warrant, or order, and regardless of whether OIG is the lead agency or assisting another law enforcement agency. See also § IX.
- C. BWCs have a limited battery life. The team leader or designated on-site supervisor may authorize SAs to deactivate their BWCs and place it in the Ready/Buffering mode if an activity that must be recorded is of such a duration that BWCs must be deactivated to conserve power. In such cases, the SA will activate the BWC and commence recording again upon direction of the team leader or designated on-site supervisor, or when safe and practical in the event of an unanticipated or exigent situation in accordance with § VI.I.
- D. SAs shall wear BWCs externally on the front of their ballistic vest carrier or outermost garment in accordance with training to ensure the best possible field of view. SAs should ensure BWCs are not obstructed by clothing, lanyards, accessories, etc. However, SAs should not alter safety principles to accommodate BWC recording. SAs should seek cover and concealment if needed and use proper tactics to ensure their safety while wearing BWCs, even if doing so obstructs the BWC recording.
- E. SAs may deactivate or turn the BWC off and temporarily remove it while attending to a personal matter, such as using the restroom, that takes them away from a recorded operation. In such cases, before resuming participation in the operation, the SA must reattach the BWC to their outermost garment and either activate it and start recording again or place it in the Ready/Buffering mode as required by this policy.

- F. If a BWC recording is stopped due to a limitation or exception (see § VII), the SA may use audio-only recording with the BWC, Axon Capture, or another audio recording device if feasible and if audio-only recording would resolve the recording concern. In such cases, the SA must resume full video recording with the BWC once the limitation or exception no longer applies.
- G. If an SA becomes aware they did not activate BWC in accordance with this policy, or it was accidentally or inadvertently deactivated during an event being recorded, they must activate the BWC as soon as it is safe and practical to do so. If this occurs, the SA must follow the procedures for an unplanned policy deviation in § VIII.B.
- H. If an SA is injured, incapacitated, or otherwise unable to operate the BWC, a supervisor or other available SA will retrieve the BWC, deactivate recording, and turn the power off. In such cases, the retrieving supervisor or SA will document actions taken in an MOA in the OCF.
- I. If an unanticipated or exigent situation arises when an SA is wearing a BWC that could result in the use of physical force or deadly force, the SA must activate and record with their BWC when it becomes safe and practical to do so. SAs should not compromise their safety or the safety of other persons to record an incident. An SA's determination as to whether the use of physical force or deadly force could arise is dependent on their training, experience, and judgement in the given circumstances. If this occurs, the SA must document the circumstances that prevented or delayed recording in an MOA in the OCF.
- J. SAs may use their BWC or an associated application such as Axon Capture to record the following evidentiary items:
 - 1. In-person or telephone interviews of witnesses, victims, subjects, or targets;
 - 2. Custodial interviews (see <u>OI Manual</u>, § 5.29 Use of Recording Devices);
 - 3. Undercover telephone calls;
 - 4. In-person or telephone interviews relating to internal or administrative investigations; or
 - 5. Other evidentiary audio, video, or still images.

VII. LIMITATIONS AND EXCEPTIONS TO BODY-WORN CAMERA RECORDING

- A. SAs will not intentionally record the following during operational activities (e.g., arrests, search warrants, seizure orders) unless unavoidable to comply with the recording requirements of this policy:
 - 1. Undercover activities or when working in an undercover or covert status;
 - 2. Confidential informants, cooperating witnesses, or sources of information;

- 3. On-scene actions by any non-law enforcement persons who are assisting law enforcement personnel prior to or after the operation; and
- 4. Medical treatment of OIG SAs or other law enforcement personnel.
- B. SAs are prohibited from recording strip searches or body cavity searches.
- C. SAs are prohibited from recording in a sensitive area in an OIG facility as designated by the SAC or SAC's designee, e.g., a secure evidence room.
- D. SAs will not use BWCs to record the following, either openly or surreptitiously:
 - 1. Non-operational conversations among OIG or other law enforcement personnel;
 - 2. Conversations between supervisors and subordinates, or conversations relating to personnel matters including performance evaluations, discipline, or counseling;
 - 3. While in a locker room or restroom in an OIG facility, or while using any restroom;
 - 4. While attending internal OIG meetings, other law enforcement meetings, or meetings with prosecutors; and,
 - 5. Operational briefings or other meetings to discuss investigations, tactics, or procedures.

NOTE: The prohibition on recording conversations does not include communications taking place during an enforcement activity that must be recorded under this policy.

E. Generally, SAs will not record with BWCs in federal, state, or local government facilities that prohibit recording. In such cases, the case agent will document the reason BWCs were not used in an MOA in the OCF. If the OIG supervisor believes circumstances exist that justify recording with BWCs in a federal, state, or local government facility that prohibits recording, the supervisor will follow the procedures in Section VIII.A to request a pre-approved deviation from the BWC policy.

NOTE: This limitation on use of BWCs applies only to federal, state, or local **government** facilities that prohibit recording. SAs will use their BWCs in accordance with this policy in all private or non-governmental locations regardless of any recording prohibition.

F. If a SAC believes BWC recording during a planned operation may be insensitive, inappropriate, or prohibited by privacy laws or regulations, the SAC may request a pre-approved deviation from the BWC recording policy if other means are inadequate to satisfy the concern (e.g., restricted access to the BWC recording). See § VIII.A. In such circumstances, the SAC may request to record audio only with BWCs if doing so would resolve the concern.

- G. If an SA deactivates the BWC during an event due to a recording limitation, exception, or prohibition, the SA must immediately reactivate the BWC and record once the limitation, exception, or prohibition no longer applies, and continue recording until deactivation is permitted under this policy. If safe and practical, the SA should state the time, time zone, and reason for deactivating, and the time upon reactivating.
- H. If, while recording operational activities (e.g., arrests, search warrants, seizure orders), an SA unintentionally or unavoidably records prohibited activities or persons, records in a prohibited location, or becomes aware that any portion of a BWC recording could reasonably be expected to constitute an unwarranted invasion of personal privacy, the SA or a supervisor must submit an Evidence Action Request to the Program Manager as soon as possible requesting the Program Manager to restrict access to the recording.

VIII. DEVIATION FROM BODY-WORN CAMERA POLICY

- A. **Pre-Approved Deviations**. The following steps apply to obtain approval for a pre-approved deviation from the BWC policy.
 - If a SAC believes there should be a deviation from OIG BWC policy for any planned operation, or if a prosecutor or other law enforcement agency requests a deviation from OIG policy, the SAC must submit a written request for a pre-approved policy deviation. In the request, the SAC will: (1) specify the policy provision(s) that will not be followed; (2) explain the reasons for the request; and (3) state whether the assigned prosecutor concurs with the request.
 - The SAC will forward the written request through the chain-of-command to the DIGI or designee. The DIGI or designee, in consultation with OC, will issue a written approval (including any conditions for approval) or denial of the request. The DIGI may also refer the request to the Principal Deputy Inspector General (PDIG) or the Inspector General (IG) for a decision.
 - 3. If approved, the case agent or SAC will document the approval in <u>Form FH6-2</u> <u>Operational Plan</u>. The case agent or SAC will add the written request and approval to the OCF.
 - 4. In compelling circumstances when there is insufficient time to submit a written request for a pre-approved deviation, the SAC may seek verbal approval from the DIGI or designee. If verbal approval is granted, the SAC will document the request and approval in an MOA in the OCF.
- B. Unplanned Deviations. The following steps will be taken if an unplanned deviation from policy occurs. This includes a failure to activate or deactivate the BWC in accordance with policy, a failure to record as required due to a device malfunction, user error, unavailability of an operable BWC, or other circumstances resulting in a deviation from the BWC policy.

- 1. An SA involved in an unplanned deviation from policy must document the circumstances in an MOA and submit it to the SAC overseeing the operation through the OIG designated onsite supervisor. If the SAC was involved in the policy deviation, the SAC will submit the MOA to the next-level supervisor.
- 2. In the MOA the SA must state the specific policy provision(s) that were not followed and explain the circumstances that resulted in a policy deviation. If the deviation involved a failure to record, the SA must explain why the recording was not made or why it was interrupted or otherwise incomplete. The SA will identify the supervisor who authorized the unplanned deviation if applicable.
- 3. The case agent or SAC will add the MOA to the OCF.

IX. JOINT OPERATIONS

- A. SAs must comply with the OIG BWC policy when operating with other law enforcement agencies unless authorized otherwise.
- B. The OIG case agent or designee will be the team leader for OIG BWC purposes for every enforcement operation.
- C. When planning an OIG-led enforcement action with another law enforcement agency, the operation team leader will discuss BWC use during the joint operation with the partner agency's team leader. The OIG team leader will brief the partner agency on OIG BWC policy and review the partner agency's BWC policy, if applicable. The case agent will document these discussions in the OIG Operational Plan, <u>FH6-2</u>. If circumstances do not allow for the OIG BWC policy briefing to be documented in the OIG operational plan, the case agent must document the briefing in an MOA added to the OCF.
- D. The OIG team leader must notify the SAC of any unresolved conflicts with other law enforcement agencies regarding use of BWCs as soon as the conflict becomes known. The SAC must then notify the DIGI or designee of the unresolved conflict. If the SAC believes there should be a deviation from OIG policy to resolve the conflict, the SAC will follow the procedures for a pre-approved policy deviation in § VIII.A. If the unresolved conflict results in a policy deviation under circumstances that do not permit a request for a pre-approved deviation, the SAC will follow the procedures in § VIII.B to document an unplanned policy deviation.

X. BODY-WORN CAMERA PROCEDURES

A. SAs must ensure their BWCs are available and fully charged before deployment. SAs will periodically check their BWCs to ensure they are functioning properly, especially during extended periods of non-use. Whenever an SA determines an assigned BWC is malfunctioning or otherwise inoperable, the SA will notify their SAC and the Program Manager and arrange to get a replacement BWC as soon as possible.

- B. SAs will check their assigned BWCs to ensure they are working properly prior to an operation that requires BWC recording. If it is not working, or if a BWC is otherwise unavailable, the SA must notify their supervisor and attempt to replace the BWC before the operation commences. If a replacement BWC is not readily available and the supervisor determines that delaying the operation to replace or repair the BWC is not practical or would impair the operation, the supervisor may authorize the SA to participate in the operation without using a BWC. In such cases, the SA will follow the procedures in § VIII.B to document an unplanned policy deviation.
- C. During pre-operation briefings, supervisors will remind SAs required to use BWCs to record and to cease recording in accordance with this policy.
- D. Supervisors will ensure that law enforcement personnel and other first responders participating in the operation (including non-OIG personnel) are informed that OIG BWCs will record the operation.

XI. POST-RECORDING PROCEDURES

- A. Applicability. The following procedures apply to OIG BWC recordings and to other OIG digital evidence made with associated Axon applications, e.g., Axon App, Axon Capture (collectively referred to as "BWC evidence"). For additional guidance on these procedures, or guidance regarding other digital evidence stored in the DEMS, see <u>OI Manual</u>, § 8.10 Digital Evidence Management System, and the <u>BWC-DEMS User Guide</u>.
- B. **DEMS Metadata**. The information entered in DEMS becomes part of the metadata connected to the evidence and is included the audit trail, including changes, edits, and deletions. All metadata and audit trails in DEMS may be subject to disclosure or release demands.
- C. Creating a Case in DEMS. Prior to uploading BWC evidence to the DEMS, SAs must create a case in the DEMS with the applicable OIG case number entered in the CASE ID field. If circumstances prevent creation of a case in the DEMS prior to uploading evidence, the SA must create the case as soon as possible thereafter. For guidance on this procedure see the <u>BWC-DEMS User Guide</u>.

NOTE: The OIG case number must be entered in the CASE ID for the DEMS to sync with the OCF in the CMS.

D. Uploading. SAs must upload BWC evidence to the DEMS as soon as possible, and no later than 72 hours after the recording was made. If the SA is unable to upload the evidence within 72 hours, e.g., due to technical issues with the BWC, inability to connect to the DEMS, or other circumstances, the SA must safeguard the BWC as evidence and upload the recoding as soon as possible.

- E. **Categories and Tagging**. Within ten days of uploading BWC evidence to the DEMS, the SA must complete the following fields and actions in the DEMS unless the specific item is listed as "optional":
 - 1. **ID**: Enter the OIG case number (mandatory).
 - 2. **TITLE**: Enter a title for the evidence item (mandatory).
 - 3. **CATEGORIES**: Add one or more categories as appropriate. See Appendix A for a list of categories, their definitions, and access classes (mandatory).

NOTE: The DEMS is configured to prevent OIG personnel from using a category unless they are members of a group that has access to items in that category.

- 4. TAGS: Enter one or more tags (optional).
- 5. **DESCRIPTION**: Enter the specific address where the activity occurs, including street address, apartment number or office number (if applicable), city/town, state, and zip code (mandatory). Entry of additional information in this field is optional.
- 6. **NOTES**: Enter notes about the evidence (optional).
- 7. Add the evidence to the appropriate case in the DEMS (mandatory).
- F. **Supervisory Responsibilities**. In the event an SA is injured or otherwise unable to upload BWC evidence, the SA's supervisor is responsible for uploading the evidence and adding the above information or arranging for it to be done by submitting an Evidence Action Request to the Program Manager. In such cases, the supervisor will document actions taken in an MOA in the OCF.
- G. **Deletion of Non-Evidentiary Accidental BWC Recordings**. If an SA accidentally or inadvertently activates a BWC recording unrelated to any case, investigation, or operational activity, the following procedure will apply.
 - 1. SAs will categorize the recording as an "Accidental Recording," and send an email to the SAC requesting deletion of the accidental recording.
 - 2. The SAC will review the recording and ensure it is not evidence. If the SAC agrees it is not evidence, they will confirm this in an email to the Program Manager requesting deletion of the accidental recording.
 - 3. Upon receiving the email request, the Program Manager will restrict access to the recording and take such steps as are necessary to confirm it is not evidence. The Program Manager may consult OC or other OIG employees as necessary on this. After completing this process, the Program Manager will refer the matter by email to the DIGI or designee with a recommendation for approval or denial of the deletion request.

The DIGI or designee will then either approve or deny the deletion request in an email to the Program Manager, who will execute the decision made in the DEMS, and add all email or other documentation to the Administrative BWC-DEMS file.

NOTE: The Accidental Recording category cannot be used for inadvertent, accidental, or unintentional BWC recordings during operational, enforcement, or investigative activities, including recordings made in the presence of a prisoner or detained person. Such recordings constitute evidence even if recorded accidentally or outside the OIG recording policy. In such cases, the SA will use the most appropriate evidence category from Appendix A, add the recording to the appropriate case in the DEMS, and if applicable, follow the procedures in § VIII.B to document an unplanned policy deviation.

Example: An SA searching a premises pursuant to a search warrant accidentally activates recording during the search after the scene is secured and recording should cease under the BWC policy. Even though the recording was accidental, it is evidence and will not be deleted.

XII. REPORTING BODY-WORN CAMERA USE

- A. SAs will note the use of BWCs in the following documentation and add it to the OCF:
 - 1. If one is completed, an MOA describing the recorded event;
 - 2. Form FH6-2 Operational Plan and Form FH6-2A BWC Post-Operational Report;
 - a. The SA completing a Form FH6-2 Operational Plan will document planned BWC use where indicated on the form.
 - b. Within ten days of the operation the Team Leader or other SA will complete the indicated portions of the <u>Form FH6-2A BWC Post-Operational Report</u> and forward it to the Program Manager.
 - c. Within ten days of receiving the BWC Post-Operational Report the Program Manager will review the BWC recordings, complete the indicated portions of the Report, and return the completed Report to the Team Leader.
 - d. The Team Leader or case agent will ensure the completed <u>Form FH6-2 Operational</u> <u>Plan</u> and <u>Form FH6-2A BWC Post-Operational Report</u> are added to the OCF.

NOTE: If circumstances do not allow for the completion of an operational plan, the case agent must document BWC use on an MOA in the OCF.

- 3. Form FH7-6 Arrest Report;
- 4. Form FH3-1 Report of Shooting/Use of Force;

- 5. MOA documenting a critical incident as defined by <u>OI Manual</u>, § 4.1;
- 6. MOA documenting a line-of-duty injury as defined in <u>OI Manual</u>, § 4.1.6.1;
- 7. An ROI or other report completed by Use of Force Report Committee regarding a critical incident (see <u>OI Manual</u>, § 4.2.3 Use of Force Review Committee (UFRC));
- 8. Whenever otherwise required in OIG policy; and
- 9. Upon direction of a supervisor.

XIII. BODY-WORN CAMERA PROCEDURES FOR USE OF FORCE CRITICAL INCIDENTS

NOTE: Due to the circumstances of a use of force critical incident, e.g., the unavailability of an uninvolved, non-witness, or uninjured OIG supervisor or SA, it may not be possible to follow every step in this section. In such cases, supervisors and SAs will follow their best judgement to ensure that BWCs and BWC evidence are accounted for and properly secured. SAs and supervisors will document unplanned policy deviations in accordance with § VIII.B.

- A. SAs will follow standard policies and procedures for use of force critical incidents. For additional information see <u>OI Manual</u>, Chapter 4 Use of Force Critical Incident Response, and the <u>BWC Critical Incident Checklist</u>.
- B. The involved OIG SA(s) and any OIG SA(s) who witnessed the incident will give their BWCs to the on-scene OIG supervisor as soon as possible after the incident. If the OIG onscene supervisor is involved in or witnessed the critical incident, the SA(s) will give it to the next most senior OIG SA on scene. If all present SAs were involved in or witnessed the incident, SAs will give the BWCs to an uninvolved OIG supervisor or SA.

NOTE: In some cases, it may be necessary to deviate from this procedure. For example, if the BWC was inadvertently detached from the SA during the incident, or if it may have physical or trace evidence (e.g., fingerprints, blood, DNA), a different procedure may be required. In such cases, the BWC should be photographed in place before removal from the scene and may require special handling and packaging to preserve any physical/trace evidence, and for processing by a qualified crime laboratory. OIG personnel should consult with the responding crime scene personnel to determine the best method of collecting and packaging the BWC, and obtaining the recording in a manner that will preserve evidentiary integrity.

C. The on-scene OIG supervisor or senior SA present will ensure that an SA responds to the hospital to retrieve a BWC assigned to an injured SA who has been removed from the scene for medical treatment or arrange for the investigating law enforcement agency to retrieve the BWC if no OIG SAs are available. The supervisor or SA who retrieves the BWC at the

scene or receives it from the investigating law enforcement agency will handle it in accordance with this policy and document the retrieval in an MOA in the OCF.

D. OIG personnel will not surrender OIG BWCs to any non-OIG agency or investigating authority. However, if an involved or witness SA is directed by the law enforcement agency investigating the incident to surrender their BWC, the SA will turn over the BWC, notify the regional OI supervisor as soon as possible, and inform them of the identity and agency of the law enforcement officer to whom it was surrendered. The SA will also document this in an MOA in the OCF.

NOTE: Only OIG can upload the BWC recordings to the DEMS. OIG will provide the relevant BWC recording(s) to the investigating authority and assigned prosecutor.

- E. The supervisor or other OIG SA retrieving BWC(s) will document the retrieval of the BWC(s) in an MOA in the OCF and include the following information in the MOA:
 - 1. The identity of the SA(s) from whom the BWC(s) were taken or the law enforcement officer who retrieved and turned them over to OIG;
 - 2. Serial number(s) of the BWC(s) taken;
 - 3. Date, time, and location the supervisor or SA took possession of the BWC(s);
 - 4. The identity of the person receiving the BWC(s) from the supervisor or SA, and the date, time, and location it was turned over, if applicable; and
 - 5. If applicable, a statement documenting that the BWC(s) were secured as evidence (see § XIII.G).
- F. The supervisor or other OIG SA retrieving FHFA-BWCs, or other assigned OIG employee, will upload the BWC recordings to the DEMS as soon as possible.

NOTE: The permissible 72-hour period to upload BWC recordings does not apply to BWC recordings involving use of force critical incidents. OIG personnel must upload BWC recordings involving critical incidents to the DEMS as soon as possible.

- G. After the BWC recording(s) are uploaded to the DEMS, an OIG supervisor or other assigned OIG employee will secure the BWC(s) as evidence following the procedures in <u>OI Manual</u>, Chapter 8 Evidence. The BWCs will remain secured as evidence pending further direction of the DIGI or designee.
- H. Once the BWC recording(s) are uploaded, the Program Manager, a System Administrator, or a Headquarters management official will add the "Critical Incident" category to the BWC recordings in the DEMS as soon as possible, which will restrict access to designated Headquarters officials. The DIGI or designee may authorize access to additional OIG personnel as needed (e.g., OC).

XIV. ACCESS, REVIEW, COPYING, AND SHARING OF BODY-WORN CAMERA RECORDINGS AND ASSOCIATED DATA

- A. All access, review, copying, and internal or external sharing of BWC recordings and associated data by OIG employees will be for official purposes only.
- B. The Program Manager will configure the DEMS to allow or restrict access to the various categories of BWC recordings as directed by the DIGI or designee.
- C. The DIGI or designee may direct restricted access to any individual BWC recordings, or they may be restricted at the request of a SAC, Headquarters management officials, or OC.
- D. Special Agent Access. Unless stated otherwise in this policy (e.g., restricted or confidential BWC recordings), SAs may access their own BWC recordings and other BWC recordings associated with assigned cases to perform the essential functions of their position. SAs may review BWC recordings for the purpose of drafting an MOA describing an activity or preparing for testimony. The purpose of using BWC recordings for these activities is to maximize the accuracy of the report or testimony, not to replace the SA's independent recollection and perception of an event.
- E. **Supervisory/Management Review**. Supervisors and Headquarters managers may review their own and their subordinates' unrestricted BWC recordings when relevant to their supervisory or management duties. Such duties include preparing for after-action debriefings, reviewing MOAs and other reports, investigative coordination, auditing compliance with the BWC and other OIG policies, and training.
- F. Sharing Unrestricted BWC Recordings. SAs and supervisors may share unrestricted BWC recordings internally within OIG and externally (e.g., other law enforcement agencies, prosecutors) for official purposes.
- G. **Prosecutor Access and Review**. OIG SAs must provide the assigned prosecutor with **all** BWC evidence relevant to a case. This includes BWC evidence that is restricted or confidential in the DEMS.
 - 1. If the BWC evidence required by the prosecutor is restricted or confidential, a SAC or higher-level authority must submit an Evidence Action Request to the Program Manager for approval by the DIGI or designee. The DIGI or designee will review the request and determine if additional arrangements should be made with the prosecutor to prevent unauthorized disclosure of the evidence.
 - 2. After any additional arrangements are made, the DIGI or designee will direct the Program Manager or other assigned OIG employee to provide the evidence to the prosecutor and ensure that the request and approval are added to the OCF. See also, § XV.C.

- H. Sharing or Copying BWC Recordings on Removable Media. OIG personnel should use the DEMS whenever possible for internal and external sharing of BWC recordings and avoid making copies on removable media. This will ensure the accountability, chain-of-custody, and audit features in the DEMS will continue to apply.
 - 1. **Unrestricted BWC Recordings**. A SAC or higher-level authority may authorize an SA to make copies of unrestricted BWC recordings on removable media if necessary for official purposes. The SAC must document the authorization in an MOA or email in the OCF.
 - 2. **Restricted and Confidential BWC Recordings**. The DIGI or designee must approve all internal and external sharing or copying of restricted or confidential BWC recordings. OIG personnel wishing to share or copy restricted or confidential BWC recordings must submit an Evidence Action Request to the Program Manager for approval by the DIGI or designee.
- I. **Training Access**. OIG employees may request access to BWC evidence to assist training activities by submitting an Evidence Action Request to the Program Manager for approval by the DIGI or designee. If the requested recording is non-evidentiary (e.g., a BWC recording made during a training activity and not associated with a case), the employee will send the request to the Program Manager by email. The Program Manager will add the request and response to the Administrative BWC-DEMS file.
- J. Access to BWC Recordings Involving Internal or Administrative Investigations. The following applies when SAs are the subject of an internal or administrative investigation related to an activity recorded by a BWC.
 - 1. The DIGI or designee may direct that the access level to the relevant BWC recordings be set at the confidential level with access granted only to designated OIG employees.
 - 2. Upon authorization of the DIGI or designee, OIG personnel conducting an internal or administrative investigation may review relevant BWC recordings prior to interviewing witness(es) or subject(s) of the investigation.
 - 3. SAs who are the subject of an internal or administrative investigation and their attorney may review their own relevant BWC recording(s) prior to being interviewed by OIG or non-OIG investigative personnel investigating allegation(s), subject to the following conditions.
 - a. The case agent or supervisors will submit an Evidence Action Request to the Program Manager for approval of the DIGI or designee to authorize the review. The DIGI or designee may consult with OC in reviewing the request. If there is a parallel criminal investigation, the DIGI or designee will ensure consultation and coordination with the assigned prosecution.

- b. Once approved, the SA and their attorney will review the BWC recording(s) in an OIG facility or other government office under controlled circumstances that do not permit reproduction of the recording(s) by any means.
- c. OIG will provide a copy of the BWC recording(s) to the SA and their attorney only with the written approval of the DIGI or designee after consultation with OC. The case agent or supervisor will add the written approval to the OCF.
- K. Use of Force Critical Incidents. The following applies when SAs are involved in or witness a use of force critical incident recorded with BWCs.
 - SAs will follow OIG policies and procedures for use of force critical incidents, including providing public safety and scene management information. See <u>OI Manual</u>, § 4.1.1 SA Responsibilities.
 - 2. All use of force critical incidents including SA-involved shootings are presumed to be under criminal investigation unless and until the relevant prosecutorial office(s) has declined prosecution. This policy does not presume the SA is the target of the criminal investigation. See § XIII and <u>OI Manual</u>, Chapter 4 Use of Force Critical Incident Response, for further guidance.
 - 3. SAs who are involved in or witness a use of force critical incident and their attorneys may review their own relevant BWC recording(s) prior to being interviewed by the investigating authority subject to the following conditions.
 - a. The PDIG or IG must authorize the review after OIG consultation with the investigating agency and assigned prosecutor on the timing, location, and conditions of the review.
 - b. The SA and their attorney will review the BWC recording(s) in a law enforcement or other government facility under controlled circumstances that do not permit reproduction of the recording(s) by any means, as mutually agreed upon by OIG, the investigating agency, and the assigned prosecutor.
 - c. OIG will provide a copy of the BWC recording(s) to the SA and their attorney only with the written concurrence of the assigned prosecutor.
- L. Audit Trails. BWCs and the DEMS produce multiple audit trails, including a BWC (device) Audit Trail, a User Audit Trail, and an Evidence Audit Trail. The Program Manager will configure access to audit trails in the BWC-DEMS System as directed by the DIGI or designee. OIG personnel may request access to case-related audit trails by submitting an Evidence Action Request to the Program Manager for approval by the DIGI or designee. If the audit trail relates to a non-evidentiary BWC recording unrelated to a case, the employee will send the request to the Program Manager by email. The Program Manager will add the request and response to the Administrative BWC-DEMS file.

XV. DISSEMINATION AND REDACTION OF BWC RECORDINGS

A. Status of BWC Recordings. BWC recordings constitute investigative information and shall be treated as law enforcement sensitive, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings. The BWC recordings are evidence in federal investigations subject to applicable federal laws, rules, and policy concerning disclosure or dissemination, including but not limited to Title 12, Subchapter A, Part 1215 of the Code of Federal Regulations (Touhy Regulations); and therefore, are deemed privileged absent appropriate redaction prior to disclosure or dissemination. Non-evidentiary accidental recordings (see § XI.G) and BWC recordings created for training and other non-investigative purposes are not subject to this paragraph.

B. Redactions

- Redactions to BWC recordings will vary based on several factors, including the type of legal proceeding (e.g., criminal, civil, or administrative), the basis for the release (e.g., criminal discovery, Freedom of Information Act (FOIA) request, etc.), the status of the case, and the contents of the specific BWC recording. The <u>BWC-DEMS User Guide</u> provides additional guidance on redactions.
- 2. SAs should consult with the prosecutor or other government attorney responsible for the matter to determine appropriate redactions. SAs should also consult OC on redaction questions and request OC assistance for unresolved redaction issues.
- 3. SAs are generally responsible to redact BWC recordings as needed for their assigned cases. When necessary, SAs may request that the Program Manager assist with redactions.
- 4. The Program Manager or other designated Headquarters employees will redact BWC recordings to be publicly released relating to a use of force critical incident under the direction of DIGI or designee. See § XVII.
- C. **Prosecutor Access to Unredacted BWC Recordings**. During an OIG investigation or a prosecution relating to an OIG investigation, the DIGI or designee may authorize disclosure of unredacted BWC recordings to an assigned prosecutor subject to the following conditions.
 - 1. Any portions of the BWC recording (video, audio, and/or metadata) that could reasonably be expected to identify a confidential informant or an undercover law enforcement officer must be redacted prior to disclosure to the prosecutor. These redactions will be made whether the prosecutor is requesting the recordings for their own use or for release under the Federal Rules of Criminal Procedure (e.g., Rule 16, the Jencks Act, Brady, and Giglio) or other federal, state, or local authorities or court rules applicable to the legal action.

- 2. OIG will maintain ownership and control over unredacted or partially redacted BWC recordings.
- 3. Due to the capabilities of the DEMS (e.g., the capability to restrict downloading and resharing, and the audit trail), SAs should use the DEMS to share unredacted or partially redacted BWC recordings with prosecutors unless not feasible.
 - a. If the recording cannot be shared through the DEMS, it may be loaded to removable media. See § XIV.H.
 - b. SAs must mark all removable media containing BWC recordings "LAW ENFORCEMENT SENSITIVE–PROSECUTION COPY–Not for Dissemination or Discovery" and keep the removable media secure from unauthorized access.
- D. **Review of Unredacted BWC Recordings by Judges**. SAs may provide unredacted BWC recordings for an in-camera review by a federal, state, or local judge upon court request or order. SAs will coordinate procedures for the review with the assigned prosecutor in criminal cases, defense attorney in civil cases, or other government attorney to ensure the unredacted recordings remain secure.
- E. **Court Orders to Release Unredacted BWC Recordings**. SACs will submit court orders to disclose unredacted recordings to parties outside OIG and motions seeking such orders to the DIGI or designee and OC. The DIGI or designee will consult with OC and the assigned prosecutor to determine whether the potential harm of disclosure is outweighed by the importance of the underlying federal or state criminal prosecution or other legal action.
- F. **Civil or Administrative Proceedings**. OIG personnel will refer requests or demands for release of BWC recordings in civil or administrative proceedings to OC for guidance and assistance.
- G. **Protective Orders**. When BWC recordings are provided to parties outside of OIG for a legal proceeding, the SA or SAC should consult with the prosecutor or other government attorney responsible for the matter and OC to determine whether a protective order prohibiting further disclosure or dissemination should be sought.

XVI. PUBLIC RELEASE OF BWC RECORDINGS

Except as set forth in § XVII, OIG personnel will handle requests for public release of BWC recordings and associated metadata and audit trails in accordance with the Freedom of Information Act, 5 U.S.C. § 552. Standard OIG FOIA policies and procedures will apply. OC manages OIG's FOIA program. OIG personnel should consult OC on FOIA questions relating to BWC recordings.

XVII. EXPEDITED PUBLIC RELEASE OF BODY-WORN CAMERA RECORDINGS INVOLVING SERIOUS BODILY INJURY OR DEATH

- A. OIG will publicly release BWC recordings that depict conduct by an OIG SA resulting in serious bodily injury or death of another, unless the IG determines specific and compelling grounds exist to justify withholding such recordings that cannot be resolved by redaction, partial withholding, or other means. BWC recordings may be withheld only upon a written approval by the IG that documents the justification for withholding.
- B. The DIGI will consult OC if there is any question as to whether an injury shown in the recorded event constitutes "serious bodily injury," and is thus subject to the expedited public release requirement.
- C. There is a presumption that OIG will review, redact, and release BWC recording(s) that show an incident resulting in the serious bodily injury or death of another as soon as practical. The following procedure for expedited public release will apply.
 - 1. The DIGI or designee will immediately notify the IG, PDIG, and the Chief Counsel of the potential expedited public release.
 - 2. Under the direction of the DIGI or designee, OI will coordinate an expedited review of the BWC recordings to determine whether public release is appropriate and what redactions are required prior to release. In making this assessment, the DIGI or designee will consult with the IG, PDIG, and Chief Counsel; the applicable United States Attorney's Office (USAO) and the responsible prosecuting office if not the USAO; any other law enforcement agency with involved personnel; and the investigating federal, state, or local agency.
 - 3. The DIGI or designee will coordinate the redaction of the BWC recordings with the SAC, Program Manager, and Chief Counsel.
 - 4. Upon completion of the review and consultation process, the DIGI will approve the request for public release of the redacted recordings, unless, in consultation with the Chief Counsel, the DIGI believes that there are specific and compelling grounds justifying denial of the request that cannot be resolved by redaction, withholding portions of the BWC recordings, or other means. In such cases, the DIGI will forward a written recommendation and justification to deny release through the PDIG to the IG for final decision.
 - 5. If the IG determines there are specific and compelling grounds to justify withholding the BWC recordings, which cannot be resolved by redaction, partial withholding, or other means, the IG will issue a written decision and justification to deny release. The DIGI or designee will ensure that the IG's written decision and justification are included in the OCF.

- 6. If the IG determines that exigent circumstances exist which necessitate accelerating the release timeline, including the need to maintain public safety or preserve the peace, OIG will devote all necessary resources to review, redact, and publicly release the BWC recordings at the earliest possible time, no later than 72 hours from the IG's determination that exigent circumstances exist. Exceptions will be exceedingly rare and must be personally approved in writing by the IG upon a finding of compelling circumstances. The DIGI or designee will ensure that the IG's written decision to delay release past 72 hours is included in the OCF.
- 7. If the request for public release is granted, the DIGI or designee will consult and coordinate the timing and manner of release with the IG, PDIG, Chief Counsel, SAC, the USAO or other assigned prosecutor, and other involved law enforcement agencies. OI and the Program Manager will provide the version of the recording(s) that will be released.
- 8. OI, OC, and Office of Chief of Staff will coordinate OIG's public response to the public release or denial.

XVIII. POLICY RETENTION

This policy belongs to the Office of Investigations and is subject to review annually or when revisions are required due to changes in law or federal policy.

APPENDIX A

BWC-DEMS EVIDENCE CATEGORIES

DEMS Category	Definition	Access Class	DEMS Retention
Accidental Recording	Non-evidentiary accidental, inadvertent, or unintentional recording.	Unrestricted	Until Manually Deleted
Arrest	Arrest or attempt to arrest including prisoner guard or transport.	Unrestricted	Until Manually Deleted
Case Closure	Added by the BWC-DEMS PM during the case closure process.	Restricted	Until Manually Deleted
Criminal Appeal	Evidence being held pending appeal of a criminal case.	Unrestricted	Until Manually Deleted
Critical Incident	Self-explanatory.	Restricted	Until Manually Deleted
Executive Hold	As directed by HQ Management.	Restricted	Until Manually Deleted
FOIA Hold	Added by the BWC-DEMS PM.	Unrestricted	Until Manually Deleted
Internal Investigation	As directed by HQ Management.	Confidential	Until Manually Deleted
Interview-Subject/Target	Self-explanatory.	Unrestricted	Until Manually Deleted
Interview-Witness/Victim	Self-explanatory.	Unrestricted	Until Manually Deleted
IT Testing	Self-explanatory. System Admins only.	Restricted	Until Manually Deleted
OC/Legal Hold	Added by the BWC-DEMS PM at request of OC.	Unrestricted	Until Manually Deleted
Other Enforcement Action	Enforcement action not covered by a more specific category.	Unrestricted	Until Manually Deleted
Pending Review	Used by BWC-DEMS PM to restrict access upon direction of HQ Management or OC or request of SAC.	Restricted	Until Manually Deleted
SA Injury	Self-explanatory.	Unrestricted	Until Manually Deleted
Search Warrant/Seizure Order	Self-explanatory.	Unrestricted	Until Manually Deleted
Shared Grand Jury Material	Grand Jury material shared with OIG by another agency only. <i>OIG grand jury material is NOT allowed in the DEMS.</i>	Confidential	Until Manually Deleted
Shared Non-Grand Jury Material	Working copies of evidence shared with OIG by another agency.	Unrestricted	Until Manually Deleted
Temporary Transcript Copy	Audio recording in the DEMS solely to produce a transcript.	Unrestricted	45 Days
Training Demo	Self-explanatory.	Unrestricted	30 Days
Use of Force	As defined by OIG policy.	Unrestricted	Until Manually Deleted