POLICIES AND PROCEDURES MANUAL

OIG 100.21

Body Worn Camera Program

1. Purpose. To establish policies and procedures for the Federal Deposit Insurance Corporation, Office of Inspector General (FDIC OIG) Body Worn Camera (BWC) program.

2. Policy. In order to enhance transparency and accountability in relation to the public trust, FDIC OIG will use BWCs during pre-planned law enforcement activities to promote the collective safety and security of the general public and government personnel at the scene, such as during the planned execution of a search warrant or arrest warrant.

3. Scope. This policy applies to the use, handling, and review of BWCs and/or BWC recordings by any FDIC OIG employee.

    a. Only Office of Investigation (OI) Special Agents (SAs) are authorized to operate a BWC.

    b. The deployment of BWCs does not supersede existing OIG OI policy regarding interviews or evidence collection (e.g., the use of surreptitious recording devices in undercover operations, the use of surreptitious recording devices in consensual monitorings, or overt recordings during interviews).

4. Authorities.

    a. Inspector General Act of 1978, as amended (IG Act);

    b. Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority, dated December 2003 (AG Guidelines);

    c. The Privacy Act of 1974, 5 U.S.C. § 552a; and

    d. Executive Order 14074 on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety (May 25, 2022).

5. Roles and Responsibilities.

    a. *Body Worn Camera Program Manager (BWC-PM).* The BWC-PM is responsible for the overall management and oversight of the BWC program, under the direction of the OI Headquarters Operations Special Agent in Charge. Among other duties, the BWC-PM will:

i. Provide daily management of the BWC program.

ii. Oversee implementation of all SA training that covers the proper use and operation of the BWC, as well as compliance with privacy and civil liberties laws.

iii. Periodically review BWC recordings to evaluate the quality of the audio and video recordings to ensure that SAs are properly operating BWCs in the manner intended by this program.

iv. Annually coordinate with the OIG-Office of General Counsel (OIG-OGC) to assist with annual privacy reviews.

v. Annually coordinate with the OIG-Office of Management (OM) to ensure compliance with record-related laws, regulations, and policies.

b. *Headquarters Operations Special Agent in Charge (HQ OPS SAC).* The HQ OPS SAC supervises the BWC program.

c. *OI On Scene Supervisor (OI-OSS).* The OI-OSS is the OI supervisor who is responsible for directing when BWCs shall be activated and when BWCs shall be deactivated on an enforcement operation. The OI-OSS typically is the on-site SAC or the lead on-site SA. This responsibility shall be discussed and identified at the pre-operational briefing. For every enforcement operation, where OI SAs are present, there shall be a designated OI-OSS.

d. *Regional Use of Force Coordinator (RUOFC).* The RUOFC is a Control Tactics Instructor (CTI), Firearms Instructor (FI), or both, who is responsible for the administration of the Use of Force (UOF) program in the region to which he/she is assigned. The RUOFC oversees the required annual (on a Fiscal Year (FY) basis) BWC familiarization training, as part of the OI firearms/UOF program, for the SAs in his/her region. RUOFCs are also responsible for ensuring that all SAs, in his/her region, receive this required annual training.

e. *Special Agents (SA).* For purposes of this policy, the term SA refers to all personnel in the 1811 job series, regardless of the titles or positions they hold.

f. *Special Agents in Charge (SAC).* The SAC is the OI regional supervisor. SACs must inventory the BWCs assigned to SAs in his/her region, at least once every FY.

6. <u>Training.</u> To ensure the proper use and operation of BWCs, as well as maintain compliance with privacy and civil liberties laws, SAs must establish and maintain proficiency and knowledge related to BWC deployment. Training for BWC deployment consists of three (3) parts:

a. *Initial Training (Use/Laws).* Prior to the deployment of BWCs, the SA must complete initial training to ensure the proper use and operation of the BWC, as well as compliance with privacy and civil liberties laws. The BWC-PM administers and/or coordinates this initial training. The BWC-PM maintains these training records per the OIG retention schedule.

b. *Annual (FY basis) Training (UOF/Firearms).* Every FY, SAs must complete BWC familiarization in conjunction with UOF training or firearms training, to maintain proficiency in the use of BWCs and ensure continued functionality of the devices. The RUOFC, for the SAs in his/her region, is responsible for coordinating and overseeing this training.

   i. The RUOFC must document this annual (FY basis) BWC familiarization training and provide a copy to the National UOF Coordinator (NUOFC). The RUOFC and NUOFC will maintain these training records per the OIG retention schedule.

   ii. If SAs are unable to complete the required scheduled training, the RUOFC shall find NUOFC approved alternative training.

   iii. If SAs fail to complete the annual (FY basis) BWC training, the RUOFC and regional SAC shall notify the Deputy Assistant Inspector General for Investigations (DAIGI) and NUOFC of the reason why primary and alternative training was not completed. The SA shall not participate in enforcement operations until this required annual training is completed.

c. *Periodic Refresher Training (Use/Laws).* SAs must receive periodic refresher training, typically during in-service training, to ensure the proper use of the BWC, as well as compliance with privacy and civil liberties laws. The BWC-PM will administer and/or coordinate this periodic refresher training. The BWC-PM maintains these training records per the OIG retention schedule.

7. BWC Equipment.

a. *Inventory Form.* After receiving initial training described above, SAs will be issued a BWC. SAs will sign an inventory form upon receipt of the BWC. This inventory form will be maintained by the applicable SAC and RUOFC for as long as the SA has the item and three (3) years after the item is no longer in the possession of the SA. The NUOFC will maintain a copy of the inventory form for as long as the SA has the item and three (3) years after the item is no longer in the possession of the SA.

b. *Inventory Report.* Every FY, the SACs will inventory all BWCs in his/her region. The SAC will complete a memorandum documenting the results and send to the HQ-OPS SAC and the BWC-PM.

c. *Use and Maintenance.* SAs shall only use BWCs issued by the OIG. SAs should exercise reasonable care when using BWCs to ensure their proper functioning. SAs should ensure that the BWC is fully charged before and during its deployment. SAs will notify the BWC-PM of any equipment malfunctions as soon as possible.

d. *Storage.* BWCs shall not be left unsecure while in the office, at home, or when traveling. Unattended BWCs shall be locked in a secure manner.

e. *Loss or Theft of Equipment.* SAs will report the loss or theft of a BWC to their SAC as soon as possible, but no later than 24 hours after the discovery of the loss or theft. The SAC shall immediately notify (in writing) the BWC-PM and the HQ OPS SAC regarding the loss/theft of the BWC.

8. <u>BWC Activation, Deactivation, and Placement.</u> SAs shall wear and activate OIG-issued BWCs for the purposes of recording their actions during enforcement operations, consistent with the guidance below.

a. *Activation of BWCs.*

i. *Enforcement operation.* BWCs shall be activated by all participating SAs upon approaching a subject or premises during an enforcement operation. The OI-OSS shall provide guidance during pre-planning briefing and during the operation regarding activation and deactivation.

ii. *Potential UOF during an enforcement operation.* If, while wearing a BWC for an enforcement operation pursuant to this policy, the BWC is approved for deactivation and an SA, thereafter, encounters an individual who is uncooperative, violent, assaultive, or discussing criminal conduct that in the SA's judgement, consistent with his/her training and experience, could lead to the use of physical or deadly force or be relevant to the investigation, the SA should activate and record with his/her BWC as soon as it is safe and practical to do so.

iii. *Interviews during an enforcement operation.* During arrests and search warrants, a BWC may be used to record an interview with an arrestee or detainee.

iv. An intentional failure to active the BWC or the unauthorized termination of a BWC recording may result in disciplinary action and/or adverse action.

b. *Deactivation of BWCs.*

i. *Enforcement Operation.* BWCs shall be deactivated by SAs only upon the direction of the OI-OSS when he/she determines, at his/her discretion, the scene is secured. For purpose of this policy, the term "secured" means that the scene is safe and under law enforcement control.

1. *Search Warrants.* When executing a search warrant, the OI-OSS may authorize SAs to deactivate their BWCs once the location to be

searched has been secured and all individuals present have been searched, as appropriate. The OI-OSS will use his/her discretion to determine when team members conducting perimeter security during the execution of the warrant may stop recording.

2. *Planned Arrests.* When executing an arrest warrant or arresting an individual during the execution of a search warrant, the OI-OSS may authorize the deactivation of most BWCs once he/she has determined the scene is secure and any arrestees are handcuffed and placed in the transport vehicle(s). While on the scene of an arrest and during prisoner transports from the scene of an arrest, SAs must continue to wear their BWCs and leave them in the Ready (Buffering) or equivalent mode.

ii. *Exceptions for Deactivation.*

1. BWCs have a limited battery life. The OI-OSS may authorize SAs to deactivate their BWCs if an enforcement operation is of such a duration that BWCs need to be deactivated to conserve power and/or for temporary storage.

2. An SA may deactivate his/her BWC at any time the SA needs to obtain emergency medical attention. Under limited circumstances, an SA may deactivate his/her BWC to attend to an urgent personal matter that takes him/her away from a planned operation, such as using the restroom.

c. *Placement of BWCs.* SAs should ensure the BWC is not obstructed by clothing or other objects. SAs should 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.

i. *BWCs with Body Armor.* If a tactical ballistic vest (body armor) is worn, the BWC will be worn on the outside/front of the body armor. Body armor is typically worn over the SA's clothing.

ii. *BWCs Without Body Armor.* In the event a BWC is deployed when body armor is not worn, the BWC will be secured to the SA's outer clothing, lanyard, or belt.

9. <u>Enforcement Operations Pre-Planning and Post Summary Activity.</u>

a. *Pre-Operation Planning and Briefings.* Prior to conducting a law enforcement operation the SA leading the enforcement operation, will adequately brief ("pre-brief") all members of the search or arrest team, detailing the planned use of BWCs. All SAs who are issued BWCs and who are expected to activate them during the enforcement operation must receive the operation briefing.

i. *Joint Operations.* When conducting enforcement operations with a partner law enforcement agency, SAs will comply with OIG's BWC policy. The SAC, overseeing the operation, shall notify the DAIGI, prior to the operation if there are any unresolved conflicts regarding the BWC deployment.

1. When conducting an enforcement operation with a partner law enforcement agency, the designated OI-OSS shall 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 OIG BWC policy and reviewing the partner agency's BWC policy, if applicable. These discussions will be documented on the Operational Plan or through a memorandum. All forms and memorandums shall be electronically maintained consistent with OI's case management policies.

ii. *Undercover Personnel.* As applicable, the operational briefing shall include a discussion of any steps that can be taken to avoid recording undercover personnel. Special care should be taken to resolve any issues related to undercover personnel.

b. *Post-Operational Summary- Documentation of BWCs.*

i. Upon the conclusion of the enforcement operation, the case agent prepares a Post-Operational Memorandum of Activity (MOA) summarizing the operation within five (5) business days of the operation. If there is a failure or malfunction with any of the BWCs, it shall be documented in the Post-Operational MOA. The Post-Operational MOA, and any other documentation, should be electronically maintained consistent with OI's case management policies and provided to the BWC-PM. Examples of BWC failures or malfunctions include:

1. The names of the team members participating in the operation;

2. Whether or not all SAs were wearing BWCs during the operation;

3. If identified/known, whether or not all BWCs were activated prior to the operation;

4. If identified/known, if any BWCs malfunctioned or were inoperable during the operation;

5. If identified/known, if any BWCs were not activated prior to, or during, the operation;

6. If identified/known, if any BWCs were turned off during the operation; and

7. If identified/known, if any BWC recording was interrupted or terminated during the operation.

ii. If there are any BWCs deviations *(see section below*), the respective SA shall notify the case agent immediately and shall prepare a memorandum or email detailing this and provide to the case agent and the OI-OSS. The case agent will use this information when preparing the Post-Operational MOA.

c. *Unplanned Deviations.*

i. Any SA that experiences a deviation from policy relating to BWC activation or deactivation due to device malfunction, operator error, or other circumstances (e.g., SA fails to activate the BWC, fails to record the entire contact, or interrupts the recording*)*, shall document the deviation in a memorandum or email within 48 hours. The memorandum or email shall address:

1. Why the recording was not made;

2. Why the recording was interrupted; and/or

3. Why the recording was terminated.

ii. The SA shall provide a copy of the memorandum or email to the case agent and the OI-OSS. The OI-OSS shall provide a copy to the case agent's SAC (and the SA's SAC, if different), BWC-PM, and HQ OPS SAC. The case agent shall electronically maintain the memorandum or email consistent with OI's case management policies.

iii. The HQ OPS SAC will determine if any additional levels of OIG management need to be briefed (i.e., DAIGI and/or the AIGI).

d. *Planned Deviation.* Any planned deviation from the OIG BWC policy must be approved, in writing, by the Assistant Inspector General for Investigations (AIGI) or DAIGI with concurrence from the OIG-OGC. Any planned deviation must be documented in either a memorandum or in the operational plan and discussed at the operational briefing.

i. Under exigent circumstances, an oral authorization may be given by the AIGI or DAIGI, but must be subsequently documented in a memorandum or email within 48 hours. All documentation must be electronically maintained consistent with OI's case management policies.

10. Restrictions on Use of BWCs.

   a. *Restrictions on BWC Use.* BWCs shall only be used in conjunction with official law enforcement duties and not personal activities. Misuse of BWCs, including improper recording, improper dissemination, or tampering with data may result in disciplinary action and/or adverse action.

   b. *Prohibited Use of BWCs.* Absent approval from the AIGI, the Deputy Inspector General, or the Inspector General, in consultation with the assigned government attorney or OIG-OGC, BWCs shall not be used to record:

      i. In a detention facility, if the law enforcement operation is not taking place in the facility; or

      ii. Personnel conducting activities involving classified information. Classified materials and/or information may not be stored, processed, or transmitted on any unclassified system.

11. BWC Recordings- Treatment/Uploading/Storage/Access.

   a. *Treatment of BWC Recordings.* BWC recordings shall be treated as law enforcement sensitive 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. Nothing in this policy shall be deemed to provide a right of public access to BWC recordings. BWC recordings are controlled by, and the property of, the OIG and will be retained and managed by the OIG.

   b. *Uploading of BWC Recordings.* The BWC devices are to be preset to automatically upload the video to the supported cloud storage. The SA wearing the BWC must confirm the BWC recording has been uploaded and if not the BWC recordings will be uploaded by the SA wearing the BWC as soon as possible, usually within 24 hours. The naming convention of the BWC recording will include case number, date, SA's last name. BWC recordings will be maintained in an OI-controlled cloud storage service where they are uploaded.

   c. *Storage of BWC Recordings.* BWC recordings will be stored in an OI-controlled cloud storage service, with any vendor access logged. Each file will contain all relevant metadata, such as the date and time of the recording, the name of the 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 BWC recording is reviewed, and the name of each reviewer.

   d. *Access to BWC Recordings.* Access to the BWC recordings will be controlled by the BWC-PM. Access to stored BWC recordings will have controlled access, recorded automatically by the system software, and audited periodically by the BWC-PM to ensure that only authorized users access the BWC 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 HQ OPS SAC. This information may be discoverable and could be requested by the prosecution or the defense during court proceedings.

12. BWC Recordings-Sharing. The BWC equipment and all data, images, video, audio, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of the OIG. The BWC-PM or the HQ OPS SAC may share BWC recordings as provided below. All requests and final decisions will be maintained by the BWC-PM. No other OI 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 or his/her designee, the Deputy Inspector General, or the Inspector General, in consultation with OIG-OGC (see sharing exceptions detailed below). SAs may review their own BWC recordings, subject to the restrictions detailed below, but may not share their BWC recordings with others.

    a. *Requests for Disclosure of BWC Recordings.* All requests for disclosure of BWC information shall be submitted to the BWC-PM. All releases should be discussed and/or reviewed by OIG-OGC prior to release. If it is necessary to make redactions to the BWC footage, they will be made by the BWC-PM or the HQ OPS SAC in consultation with OIG-OGC. The BWC-PM is responsible for sharing the BWC recordings and documenting the request and action taken.

        i. *DOJ – Discovery Requests for Pending Criminal Investigations.* The BWC-PM or the HQ OPS SAC may provide a copy of a BWC recording to an assigned government prosecutor upon request. Any requests from the assigned government prosecutor shall be sent by the case agent to his/her SAC and the BWC-PM. Release of the recording will be discussed and/or reviewing with OIG-OGC prior to release.

        ii. *Partner Law Enforcement Organizations.* The BWC-PM or the HQ OPS SAC may provide a copy of a BWC recording to a partner law enforcement agency upon request and after concurrence from the assigned government attorney. Any requests shall be sent by the case agent to his/her SAC and the BWC-PM. Release of the recording will be discussed and/or reviewing with OIG-OGC prior to release.

        iii. *Freedom of Information Act (FOIA) or Privacy Act requests.* Any request for records made pursuant to FOIA or the Privacy Act received by an OIG employee must be forwarded to OIG-OGC. FOIA or Privacy Act requests for the release of BWC recordings will be forwarded by OIG-OGC to the BWC-PM, HQ OPS SAC, and the AIGI. The BWC-PM will, at a minimum, in conjunction OIG-OGC, review all BWC footage that is proposed for release and specify which parts of the footage may be released and which parts need to be redacted, along with the relevant justifications, and provide a complete copy of the BWC recording to OIG-OGC with the suggested redactions and justifications in writing. OIG-OGC will review the suggested redactions and justifications and provide its comments and/or concurrence to the BWC-PM. Upon receiving concurrence from the OIG-OGC, the BWC-PM will use the appropriate redaction software to redact the BWC recording. The BWC-PM will produce the redacted BWC recording or provide to the OIG-OGC for disclosure in accordance with FOIA and/or the Privacy Act.

iv. *All Other Requests Outside of the FDIC OIG.* Requests for OIG BWC recordings unrelated to a pending OIG criminal investigation or case will be forwarded to the OIG-OGC, which is responsible for processing and responding to such requests. OIG-OGC will coordinate with the BWC-PM who will provide necessary copies, redactions, and assist with the production of the BWC recordings (see section below). OIG-OGC will provide the BWC-PM information about the decision and actions taken in response to each request processed by OIG-OGC.

13. <u>BWC Recordings- Redacting.</u> In any situation where BWCs record content that otherwise should not be shared because of any law enforcement sensitivities or privacy concerns, which could include recordings of undercover personnel, confidential informants, sensitive investigative techniques or equipment, minors, injured or incapacitated individuals, or sensitive locations such as restrooms, locker rooms, or medical facilities, the BWC-PM and the HQ OPS SAC, in consultation with the OIG-OGC, may use redaction software to blur images or portions of images, or minimize audio content, when making copies of BWC recordings for disclosure.

    a. *Undercover Agents.* If an undercover agent participates in the operation and the SAs on the scene are not able to take measures to avoid recording the identity of the undercover agent, the OI-OSS will inform the BWC-PM and note this occurrence in writing. The BWC-PM will coordinate with the OIG-OGC on what steps should be taken, if any, to redact any images and voice recordings of any undercover personnel.

14. <u>Access and Review of BWC Recordings.</u> An SA may have access to the audio and video derived from their issued BWC when it is reasonable and necessary for the SA to perform essential functions of his/her job. This includes, but is not limited to, a review necessary to create an MOA describing a recorded operation. Requests for access for essential functions should be submitted in writing by the SA to the BWC-PM stating the reason for access. In matters where the BWC recording is relevant to an OIG management inquiry or employee investigation, access requests must be approved by the HQ OPS SAC, in consultation with OIG-OGC.

15. <u>BWC Recordings- Deleting.</u> Any request to delete a portion or portions of the BWC recordings, such as accidental recordings or trainings, must be submitted via a memorandum from the SA, through his/her SAC, and approved in writing by the AIGI or his/her designee, the Deputy Inspector General, or the Inspector General, after consultation with the OIG-OGC. The memorandum must state the reason(s) for the

request to delete the recording. If the request is approved, the written approval will be provided to the BWC-PM. The BWC-PM may delete the BWC recording only after receiving the approved requested memorandum. All requests and final decisions will be maintained by the BWC-PM.

16. <u>BWC Recordings- Training.</u> BWC recordings may be used for training purposes. Access to those BWC recordings will be coordinated through the BWC-PM. When necessary, the BWC-PM, in consultation with the OIG-OGC, will obtain the written permission of any OIG personnel whose recordings or images are depicted in any training videos.

17. <u>BWC Records Retention.</u> BWC recordings will be retained according to OIG retention policies.

    a. BWC recordings that are not associated with complaints or allegations made against OI employees and do not contain information pertinent to the case being investigated will be kept for five (5) years following case closure unless a request is provided in writing to the BWC-PM through the AIGI or his/her designee.

    b. *Statements made.* BWC recordings associated with information pertinent to the case being investigated, such a spontaneous statement of a subject/target or witness, or law enforcement officer, will be kept in accordance with OIG's retention policy. The SA will memorialize these statements (i.e., a MOA) and the document shall be electronically maintained consistent with OI's case management policies.

    c. *UOF/Complaints/Allegations*. BWC recordings associated with UOF incidents involving OI employees, complaints or allegations made against OI employees, or any other investigative matter involving OI employees, will be retained as directed by the AIGI or his/her designee in consultation with OIG-OGC.

    d. *Training.* BWC recordings associated with normal training exercises (i.e., no injuries) will be deleted after the appropriate FI, CTI, or RUOFC reviews the BWC recordings for teachable scenarios and confirms it is acceptable to delete the recording. If a teachable scenario is found, the FI, CTI, or RUOFC will ask the SA(s) involved if they would like their faces redacted and/or voices changed from the recording before its use 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.

18. <u>BWC Recordings-Expedited Public Release.</u> Following incidents involving serious bodily injury or deaths in custody, which shall be consistent with applicable law and the Privacy Act of 1974, OI shall take into account the need to promote transparency and accountability, the duty to protect the privacy rights of persons depicted in the footage, and any need to protect ongoing law enforcement operations. OIG-OGC, in consultation with the Deputy Inspector General and the Inspector General, will handle considerations related to the expedited public release of BWC recordings in this situation.

19. <u>Privacy Act Referrals.</u> The Privacy Act authorizes the OIG to refer documents and results of investigations to other law enforcement agencies. Specifically, under the current relevant system of records notice, the OIG may disclose pertinent information to appropriate Federal, State, local or foreign agencies, or other public authority responsible for investigating or prosecuting the violations of, or for enforcing or implementing a statute, rule, regulation, order, or license, where the information, either alone or with other information, indicates a potential violation of civil or criminal law or regulation, etc. Privacy Act referrals of OIG records, including BWC recordings, to another law enforcement agency must be reviewed by OIG-OGC.

20. <u>Questions.</u> Questions about this policy may be directed to the OI HQ OPS SAC.

21. <u>Effective Date.</u> This policy is effective August 24, 2022. This policy will be implemented upon procurement of all required equipment and training of staff.