OIG Manual

U.S. Department of Labor Office of Inspector General

Date: August 22, 2022

TO THE PROTECTION OF THE PROTE

Transmittal Sheet

IN 08-1900

INVESTIGATIONS: Body Worn Camera Program

This Investigative Notice (IN) prescribes U.S. Department of Labor (DOL), Office of Inspector General (OIG) policies and procedures for the use of body worn cameras.

This IN applies to the Inspector General (IG), the Deputy Inspector General (DIG), the Assistant Inspector General for Investigations (AIGI), and any OIG Special Agent in the ES/GS/GL-1811 Criminal Investigator job series in the Office of Investigations-Labor Racketeering and Fraud (OI) and the Office of Special Investigations (OSI).

There are no prior INs that address the use of body worn cameras. This IN will be effective on October 1, 2022 and will remain in effect until canceled or superseded. It requires implementation of action items and contains information of a continuing nature.

OIG Manual

U.S. Department of Labor Office of Inspector General



Investigative Notice

Chapter: INVESTIGATIONS

Title: Body Worn Camera Program

IN: 08-1900 Date: August 22, 2022

1. PURPOSE

The purpose of this Investigative Notice (IN) is to prescribe U.S. Department of Labor (DOL or Department), Office of Inspector General (OIG) policies and procedures for the use of body worn cameras (BWCs). This IN applies to the Inspector General (IG), the Deputy Inspector General (DIG), the Assistant Inspector General for Investigations (AIGI), and any OIG Special Agent in the ES/GS/GL-1811 Criminal Investigator job series in the Office of Investigations-Labor Racketeering and Fraud (OI) and the Office of Special Investigations (OSI).

2. COVERAGE

This IN shall apply to all OIG employees mentioned above, as well as to any OIG employees who obtain law enforcement powers pursuant to a U.S. Marshals Service (USMS) special deputation as a Special Deputy U.S. Marshal or other statutory authority. The terms "Special Agent" (SA) and "Agent" as used in this IN refer to anyone, regardless of rank or title, who exercises law enforcement authority pursuant to IN 08-0600, (Policies and procedures for the exercise of law enforcement powers (on and off duty), including the use of firearms, law enforcement control tactics, basic tactics, and use of force).

3. SCOPE

The use of BWCs by OIG SAs must be exercised in accordance with agency policy, U.S. Department of Justice (DOJ) guidance, and applicable laws. This policy does not govern the use of consensual monitoring, found in IN 08-0800 (Consensual Monitoring Policy), recorded interviews, found in IN 08-0900 (Interviews), or handling of evidence found in IN 08-1200 (Acquisition, Scientific Examination, Preservation and Management of Evidence).

4. BACKGROUND

The Inspector General Act of 1978 created the OIG and empowered the OIG to conduct audits and investigations relating to the programs and operations of the

Department. The IG Act further transferred the authority to conduct certain labor racketeering and organized crime investigations from the Department to the OIG.

Pursuant to the IG Act, the AIGI has the responsibility for supervising the performance of investigative activities¹ relating to the programs and operations of the Department. This investigative notice is being issued pursuant to the AIGI's investigative oversight responsibilities.

The use of BWCs by SAs fosters public trust, transparency, and accountability. BWCs enable SAs to capture contacts between witnesses, subjects, targets, and the public. This documentation can help resolve complaints made against agency personnel and possible wrongdoing by third parties. In some cases, recordings from BWCs can have evidentiary value, and may capture things that the SA did not see, hear, or otherwise notice.

5. RELATED POLICIES

- A. IN 01-0100, Electronic Case File (ECF) Management and Reporting;
- B. IN 08-0600, Policies and procedures for the exercise of law enforcement powers (on and off duty), including the use of firearms, law enforcement control tactics, basic tactics, and use of force;
- C. IN 04-0400, Use of Force (UoF) / Shooting Incidents;
- D. IN 08-0800, Consensual Monitoring Policy;
- E. IN 08-0900, Interviews;
- F. IN 08-1200, Acquisition, Scientific Examination, Preservation, and Management of Evidence;
- G. IN 08-1400, Search and Seizure;
- H. IN 08-1500, Arrests;
- I. Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety dated May 25, 2022²

6. RESPONSIBILITIES, ADMINISTRATION, and PROCEDURES

IG & DIG

- A. Responsible for the overall administration and direction of the BWC program.
- B. Responsible for approving the release of BWC footage pursuant to internal investigations and management inquiries involving OSI personnel.

IN 08-1900

¹ The Deputy Inspector General is responsible for supervising the performance of investigative activities of the Office of Special Investigations.

² Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety | The White House

AIGI and Deputy Assistant Inspector General for Investigations (DAIGI)

- A. Responsible for the overall operation of the BWC program within OI.
- B. Responsible for authorizing the use of BWCs under certain circumstances, as detailed in Sections 7.D.6) and 7.D.7).
- C. Responsible for waiving the requirement to deploy BWCs in situations when DOL-OIG is the lead investigative agency.
- D. Serves as the approving official for any proposed deletion or alteration of any BWC recording, or part thereof.
- E. Authorizes the release of BWC footage pursuant to management inquiries involving OI personnel.
- F. Coordinates production of BWC footage to the DIG and members of any involved external agency for matters involving OSI personnel.

<u>Special Agent-in-Charge (SAC), Division of Investigations and Administration</u> (DIA)

A. Responsible for Overseeing DOL-OIG's BWC program, to include creating a training program and making it available to BWC users.

BWC Program Manager (BWC PM)

A. Responsible for the daily management of the program to include addressing policy questions and BWC use.

SACs OI/OSI

- A. Responsible for ensuring SAs use BWCs in accordance with this policy.
- B. Responsible for addressing equipment issues with DIA as they arise.
- C. Responsible for appointing at least one BWC Coordinator in their area of responsibility.
- D. Responsible for ensuring BWC footage is uploaded/downloaded in accordance with policy and AIGI/DAIGI guidance.
- E. Responsible for following IGD 5-300, Policy for Handling Requests Under the Freedom of Information Act and the Privacy Act, when they receive Freedom of Information Act (FOIA) or Privacy Act requests for BWC recordings, and copying the SAC DIA and the BWC PM on the referral to the Information Disclosure Office.

SAC, Division of Advanced Technology & Analytics (DATA):

A. Responsible for maintaining a Digital Evidence Management System (DEMS) storage solution deemed appropriate by the AIGI.

- B. Responsible for ensuring the security, operability, and budgeting, of the DEMS.
- C. Responsible for providing technical support to regions when necessary.

Supervisors

A. Responsible for ensuring that all SAs attend required training on the use of BWCs and this IN.

7. PROCEDURES

A. Joint Agency Operations

- 1) SAs shall comply with this IN when conducting enforcement operations with another law enforcement agency.
- 2) Whenever possible, the DOL-OIG enforcement operation team leader shall discuss the use of BWCs with other joint agency team leader(s) prior to an operation. Ideally, this should occur at or before the operation's pre-briefing.
 - i. Situations when DOL-OIG is the Lead Agency. The regional SAC shall notify the AIGI or DAIGI if there are any unresolved conflicts with other law enforcement agencies regarding DOL-OIG deployment of BWCs during an enforcement operation when DOL-OIG is the lead agency. In instances where such a matter is unresolved and DOL-OIG is the lead agency, the AIGI or DAIGI may waive the requirement to deploy BWCs when deployment could adversely impact operational resources or relationships with partner agencies. Any such waiver shall be documented by the case agent's manager under Section 3(d) on Body Worn Camera Activity Form (OIG-292). Signed copies of OIG-292 shall be uploaded into the ECF.
 - ii. <u>Situations when DOL-OIG is not the Lead Agency</u>. DOL-OIG will make every attempt to deploy BWCs in cases where it is not the lead agency. However, when requested to not deploy BWCs by the lead agency, DOL-OIG personnel are excused from this responsibility. Any such circumstance shall be documented by the case agent's manager under Section 3(c) on the OIG-292. Signed copies of OIG-292 shall be uploaded into the ECF.

B. When to Deploy BWCs

 ENFORCEMENT OPERATIONS. SAs shall deploy BWCs during enforcement operations, such as search warrant executions and arrests. The use of BWCs will be outlined in agency operational plans and discussed during operational briefings. All DOL-OIG SAs participating in an enforcement operation will be equipped with a BWC;

- 2) <u>INTERVIEWS</u>. During enforcement operations, SAs may use BWCs to record interviews when done pursuant to IN 08-0900 (Interviews);
- 3) OTHER MISCELLANEOUS CONTACTS. SAs may request approval from their ASAC to deploy BWCs in other instances, such as a field interview of a witness with an extensive criminal history or history of violence, or in other circumstances where it may be prudent to record the contact, i.e. transporting a prisoner. When obtaining prior approval is not possible, SAs may activate their BWCs when, in their judgment, the recording of a particular interaction or activity is prudent to ensure OIG equities or officer safety.

C. Placement of BWCs

Generally, SAs shall wear BWCs externally on the front of their ballistic vest carrier or outermost garment to ensure the best possible field of view. SAs should ensure BWCs are not obstructed by clothing, lanyards, accessories, etc.

D. Activation and Deactivation of BWCs

- 1) During enforcement operations, SAs will activate their BWCs at the direction of the DOL-OIG enforcement operation team leader or designated onsite agency supervisor. It should be noted that unless otherwise ordered by the AIGI, BWCs will be configured so that upon being turning on, they record a 30-second buffer of video prior to manual activation. Generally, activation should occur prior to commencing the operational stage of an enforcement activity. Upon activation, SAs shall verbally state, "Body camera activated," his/her name, and the date and time;
- 2) To ensure the integrity of BWC recordings, the BWC must continuously operate until the activity is over, unless the SA engages in a restricted use activity, as outlined in this IN;
- 3) During enforcement operations, SAs shall deactivate their BWCs at the direction of the DOL-OIG team leader or designated onsite agency supervisor. Prior to deactivating the BWC, the SA will state "Body camera deactivated," his/her name, the date and time, and reason for deactivating, i.e., going to the bathroom, end of operation and directed by the team leader, etc. If the BWC is deactivated due to a restricted use activity as outlined below, if appropriate, the BWC must be immediately reactivated when

finished:

4) When executing a warrant, the DOL-OIG team leader or designated onsite agency supervisor can authorize the team to deactivate the BWC once the location to be searched has been secured and deemed safe. The DOL-OIG team leader or designated onsite agency supervisor will use his or her discretion to determine whether team members participating as outside cover during the execution of the warrant should continue to record. If during the execution of a warrant the team leader or site supervisor determines that a particular activity should be recorded, i.e. breaching a safe, a BWC may be reactivated until the particular activity is completed;

- 5) The DOL-OIG team leader or designated onsite agency supervisor can authorize SAs to deactivate their BWCs if an enforcement operation is anticipated to last a long time. This will conserve BWC battery life and memory storage, which is limited;
- 6) In general, BWCs should be activated during the operational stage of an enforcement activity, until the scene has been secured and deemed safe. However, SACs can seek permission from the AIGI or DAIGI to leave BWCs activated for longer durations if they believe there is an operational reason to do so. If seeking approval from the AIGI or DAIGI is not possible or is impractical, SACs may approve extended recording consistent with this policy. The DAIGI or AIGI must be notified whenever a SAC exercises this authority;
- 7) SAs equipped with BWCs should be mindful of locations where recording may be considered insensitive, inappropriate, or prohibited by privacy laws, regulation, and/or policies. BWCs shall only be used in conjunction with official law enforcement duties and not personal activities. BWCs shall not be used to record:
 - ii. Undercover operations;
 - iii. Communications with other DOL-OIG personnel taking place outside the confines of an operation or training unless approved in writing by the AIGI or DAIGI;
 - iv. Locations where individuals have a reasonable expectation of privacy such as a restroom or locker room without the permission of the AIGI or DAIGI³:
 - v. When SAs receive medical attention.

IN 08-1900

³ Subjects of arrest and occupants of a search warrant location do not enjoy any reasonable expectation of privacy during the operational phase of an enforcement activity. If for some reason BWCs are not deactivated after the scene has been secured and deemed safe, SAs may physically adjust the head of their BWC so activity requiring privacy is not captured on video. However, SAs should make every effort to continue to capture audio during this activity. Only in rare circumstances should SAs deactivate their BWCs to escort arrestee(s) and individual(s) at a search warrant location to engage in activities like using the bathroom, getting dressed, etc. Whenever possible, SAs should engage in these activities in gender appropriate pairs.

8) An intentional failure to activate a BWC or the willful or unauthorized termination of a BWC recording may result in disciplinary action.

E. Uploading and Documenting the Use of BWCs

- 1) An OIG-292 shall be completed by OIG SAs and managers following an operation where BWCs have been deployed. The case agent's manager is responsible for completing OIG-292 for occasions when their use is waived by the AIGI or DAIGI or when DOL-OIG is not the lead agency and BWCs are not deployed. Agency personnel shall follow all instructions on the OIG-292;
- 2) Barring unusual, exigent, or technical issues, all participating agency personnel are responsible for ensuring their BWC recording is uploaded to the DEMS within two business days of recording. During the same period, all participating OIG employees will complete an OIG-292 and email it to the case agent;
- 3) Barring unusual, exigent, or technical issues, the case agent will have ten business days following an operation to prepare and upload an OIG-110 Memo to File (MTF) into the ECF that provides a brief summary of the activity and identifies any issues encountered during the activity. This can be combined with other activities that are mandated by policy to be memorialized following an operation. The case agent should attach to the OIG-110 MTF any OIG-292's that were sent to him/her by participating OIG employees.

F. Storage of BWC Footage

- 1) Each BWC upload file shall contain the date and time of the recording, a unique BWC identifier, and the name of the assigned SA. An audit log is automatically created and maintained on the history of every recording. Files and folders will be named according to guidance provided by the SAC DATA;
- 2) If a UoF or other significant incident occurs during an enforcement operation or investigative activity requiring use of BWCs, the BWC recordings will be handled in accordance with section 6.E. In addition, the case agent, or in the absence of the case agent, the senior agent at the scene, will notify their SAC, who will also notify the case agent's SAC, if different from their own;
- 3) If the BWC recording is deemed evidence, the SA who deployed the BWC will coordinate with the case agent to ensure the BWC content is preserved. This shall include creation of an OIG-111 in the ECF, uploading the content in the ECF, or creating a copy outside of the ECF, e.g., burning it to digital media to be maintained in an evidence room. If needed, a working copy of the BWC recording may be provided to the case agent.

G. Records Retention and Management

BWC recordings will be securely stored on a dedicated server. All recordings are agency records and should be disposed of in accordance with DOL-OIG's records retention policy. For BWC recordings deemed as evidence, the SA will adhere to DOL-OIG's evidence policy. BWC content deemed non-evidentiary, will be treated as temporary records and maintained on the DEMS for a period of five years. On an annual basis, OI HQ will coordinate with the OIG Records Officer to properly dispose of temporary BWC files greater than five years old. Any BWC content stored outside of DEMS shall be maintained in a container that bears the proper markings related to controlled material.

H. BWC Equipment

SAs shall only use DOL-OIG-issued BWCs. SAs should exercise reasonable care when using BWCs to ensure proper functioning. SAs should ensure that BWCs are fully charged before deployment. SAs shall notify their SAC and BWC coordinator of any equipment malfunctions as soon as possible.

I. Loss or Theft of BWC Equipment

All SAs shall report the loss or theft of a BWC to their immediate supervisor as soon as practical, but within 24 hours, of the discovery of the loss or theft. The immediate supervisor shall notify the SAC. If the BWC contained footage relevant to an operation or investigative activity, the SA will detail that in a memorandum sent to their SAC. The SAC will notify the SAC DIA and the BWC PM.

J. BWC Recordings

BWC equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the sole property of DOL-OIG. SAs shall not edit, alter, erase, duplicate, copy, share, or otherwise release, disclose or distribute in any manner, any BWC recording, without prior written authorization from the AIGI or DAIGI. SAs must obtain supervisory approval prior to routine disclosure of any BWC content to law enforcement partners. Unauthorized accessing, copying, or releasing of files is strictly prohibited. Requests from third parties under section 8. below, will be handled by the Information Disclosure Office.

K. Deleting BWC Recordings from the DEMS Server

Any request to delete BWC footage, i.e. accidental or inadvertent recording, must be submitted via memorandum to the BWC PM for AIGI or DAIGI approval. The request must outline the reason(s) for the proposed deletion. Once the request is approved, it will be provided to the SAC and the OIG Records Officer. The recording may only be deleted after the requesting SAC receives the approved memorandum and concurrence is obtained from the OIG Records Officer. All documentation regarding requests and final decisions will be maintained by the BWC PM and relevant BWC Coordinator. HQ will maintain a log of deleted BWC content. BWC content made for

training and testing purposes may be deleted immediately, and maintained no longer then seven days. HQ will maintain a delete log of this content, which still requires concurrence from the OIG Records Officer prior to its deletion.

L. Access and Review of BWC Recordings

Access to BWC storage systems will be audited, quarterly by the SAC DATA and the BWC PM, to ensure that only authorized users are accessing the data for authorized purposes. Only those personnel and their managers with an official need to know who are given the appropriate permissions/assigned roles may view BWC content. Any other requests to review BWC recordings must be made in a memorandum to the BWC PM via their BWC Coordinator. The memorandum must outline the reason(s) for the request.

M. Permissible Reviews of BWC Recordings

- A SA may view BWC content taken by him/her at any time, including to defend against allegations of misconduct, inappropriate UoF, acts taken during a critical incident, or poor performance during the recorded enforcement activity. SAs will not share BWC files without an official purpose and must have prior approval of the AIGI or DAIGI to do so, unless otherwise outlined in this policy;
- 2) SAs who are the subject of a management inquiry or investigation may review his/her own BWC recording prior to providing any statements to, or being interviewed by OIG management, OSI, or other law enforcement agency. The SA may review the recording with his/her attorney or other representative;
- 3) Following a UoF or critical incident, the reviewing officials assigned pursuant to IN 04-0400 (Use of Force (UoF)/Shooting Incidents) shall be provided with copies of all relevant BWC footage. Further, the involved SA will be given the opportunity to view his or her own BWC recording prior to giving a formal statement. SAs who are witnesses to a UoF or critical incident shall also be allowed to view their own BWC recording prior to giving a formal statement;
- 4) During the course of conducting internal investigations, OSI may only review BWC recordings after opening a properly predicated case based on a credible allegation of misconduct by a SA and only in connection with that OSI investigation. OSI requests for BWC footage shall be submitted via memorandum from the SAC OSI to the DIG with a copy to the AIGI. This memorandum should, at a minimum, include what is being requested, the nature of the request, and that it is for an open OSI investigation. If the request is approved, the DAIGI will direct the BWC PM to produce the BWC content for SAC OSI. DOL-OIG officials requiring access to BWC content as part of a management inquiry shall follow the same process outlined above with the exception of sending the memorandum to the AIGI;

5) The DIG may approve the release of BWC content when a matter involves internal investigations or management inquiries involving OSI personnel. In these circumstances, the AIGI should coordinate with the BWC PM to produce relevant BWC content for both the DIG and members of an external agency, i.e., another Inspector General pursuant to guidance received from the DIG:

6) The OIG may not review BWC recordings solely for evaluating the performance of SAs during the operation or for conducting performance appraisals.

N. Training

- All SAs must attend an agency approved training program to learn how to deploy BWCs properly and to ensure compliance with this IN. Additional periodic training will be provided to ensure continued proficiency;
- 2) To ensure operational readiness and proficiency in the use of BWCs, the BWC PM and SAC DIA, will remain aware of significant issues impacting the use of BWCs, such as changes in technology and law. This may be accomplished by close liaison with federal law enforcement partners, communication with the BWC vendor, or training.

8. REQUESTS BY THIRD PARTIES

A. FOIA Requests

- 1) Recordings from BWCs may be subject to release pursuant to the FOIA. Request for records made pursuant to the FOIA received by a DOL-OIG employee shall be forwarded to the Information Disclosure Office via their SAC, with a copy to SAC DIA and the BWC PM.
- 2) The Information Disclosure Office is responsible for responding to and processing the request. The BWC PM will assist the Information Disclosure Office on the release of any BWC footage. The BWC PM will, at a minimum, provide the Information Disclosure Office relevant BWC footage that is responsive to the FOIA request. The Information Disclosure Office will determine which parts of the footage will be released and which parts should be redacted consistent with permissible FOIA exemptions and exclusions. The Information Disclosure Office will prepare a memorandum informing the BWC PM of the sections of the recording that need to be redacted. The BWC PM will use the appropriate software to redact a copy of the BWC recording. The BWC PM will then return the redacted BWC recording to the Information Disclosure Office who will review it for release under FOIA.
- 3) The U.S. Congress has provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The

provisions protecting those records are known as "exclusions." The following FOIA exclusions may exempt BWC recordings from disclosure requirements under the FOIA:

- The first exclusion protects the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings;
- ii. The second exclusion is limited to criminal law enforcement agencies and protects the existence of confidential informant records when the informant's status has not been officially confirmed;
- iii. The third exclusion is limited to the Federal Bureau of Investigation and protects the existence of foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified.

Exclusions are used very rarely and a request-by-request analysis must be conducted to determine if an exclusion applies to any particular FOIA request.

4) The U.S. Congress established certain categories of information that are not required to be released in response to a FOIA request because release would be harmful to a government or private interest. These categories are called "exemptions" from disclosures. However, even if an exemption applies, agencies may use their discretion to release information when there is no foreseeable harm in doing so and disclosure is not otherwise prohibited by law. There are nine categories of exempt information. Exemption 7 of FOIA, often referred to as the law enforcement exemption, is the most common exemption used by law enforcement. The Information Disclosure Office should be consulted for additional information on FOIA exemptions.

B. Privacy Act Referrals

- 1) The Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), provides safeguards for individuals against an invasion of personal privacy through the misuse of records by Federal agencies. The Privacy Act balances the individual's personal privacy interest against the Government's need to maintain information about individuals.
- 2) DOL-OIG is authorized under the provisions of the Privacy Act to refer documents and results of investigations to other law enforcement agencies. Specifically, under the system of records under which DOL-OIG is currently operating, DOL-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 disclosing agency (i.e. DOL-OIG), becomes aware of a potential violation of civil or criminal law or regulation, etc.

3) Disclosure of DOL-OIG records, to include BWC recordings, to another law enforcement agency must be reviewed by the Information Disclosure Office with the exception of referrals to DOJ or where there is a threat of imminent danger, or death, or physical injury.

4) Any request for records made pursuant to the Privacy Act received by a DOL-OIG employee shall be forwarded to the Information Disclosure Office via their SAC. The Information Disclosure Office is responsible for responding to and processing the request. At the request of the Information Disclosure Office, the BWC PM will assist with the release of any BWC footage. The BWC PM will, at a minimum, provide the Information Disclosure Office relevant BWC footage that is responsive to the request. The Information Disclosure Office will determine which parts of the footage will be released and which parts need to be redacted, along with the relevant justifications. The Information Disclosure Office will prepare a memorandum informing the BWC PM of the sections of the recording that need to be redacted. The BWC PM will use the appropriate software to redact a copy of the BWC recording. The BWC PM will then return the redacted BWC recording to the Information Disclosure Office who will review it for release under the Privacy Act.

C. Expedited Release of Footage

 When a request for body worn camera footage pertains to an incident involving serious bodily injury or death, the Information Disclosure Office will prioritize the request and the footage shall be released as soon as practicable consistent with this policy.

9. ATTACHMENTS

OIG Form 292, Body Worn Camera Activity Form

10. EFFECTIVE DATE

This IN is effective on October 1, 2022 and will remain in effect until rescinded or superseded.