



# Homeland Security

May 22, 2023

Policy Statement 045-07

MEMORANDUM FOR: Agency Leaders

FROM: Alejandro N. Mayorkas  
Secretary

A handwritten signature in blue ink, appearing to read "AN Mayorkas", is written over the "FROM:" field.

SUBJECT: **Department Policy on Body Worn Cameras**

## I. Purpose

Pursuant to the Secretary's authority under Title 6, United States Code (U.S.C.) § 112, this policy articulates Department-wide standards and guidelines related to body worn cameras (BWC) used by Department of Homeland Security (DHS) law enforcement officers and agents (LEOs). All DHS Agencies and Offices employing LEOs (hereafter "Agencies") are directed to implement this policy through Agency-specific policies, procedures, and training. In general, this policy will serve as the enterprise-wide standard for DHS LEOs and Agencies, including within interagency environments.

## II. Use of BWCs

A. BWCs are to be used for purposes of recording a LEO's interactions with the public in the following situations:

1. As defined by Agency policy, in all appropriate circumstances when LEOs are conducting patrol or are otherwise engaged with the public in response to emergency calls;
2. During 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; or,
3. During the execution of a search or seizure warrant or order.

B. BWCs shall not be used:

1. For the sole purpose of recording individuals who are engaged in activity protected by the First Amendment, e.g., people who are lawfully exercising their freedom of speech, press, association, assembly, religion,

or the right to petition the government for redress of grievances. This prohibition does not preclude use of BWCs for situations while the LEO is otherwise addressing potentially unlawful activity or the BWC is engaged pursuant to one of the requirements set forth as described above in Section II(A). Furthermore, BWCs shall not be used for systemic, indiscriminate tracking of individuals, wide-scale monitoring, or unauthorized surveillance.

2. In the following environments unless the LEO is engaged in Section II(A) activities set forth above:
  - Courtroom during proceedings;
  - Hospital or medical facility; or,
  - Any location where there is a reasonable expectation of privacy.
3. For the sole purpose of recording undercover personnel, confidential informants, confidential sources, or any undercover activity.
4. Solely for conducting or supporting a personnel investigation, disciplinary action, or employee performance assessment. This prohibition does not apply to student-instructor feedback in a BWC training environment that is otherwise recorded in accordance with established Agency policy.
5. For the purpose of recording a particular individual or group of individuals based solely on their race, color, religion, national origin,<sup>1</sup> sex, age, disability, sexual orientation, marital status, parental status, gender identity or expression, or political affiliation.
6. For the purpose of recording an activity with a LEO's BWC if doing so places the LEO in a situation that could result in physical injury to the LEO or others.

### III. Agency Requirements

#### A. Agency Policies

1. Agencies are directed to develop, or update, policies to address the content of this policy within 180 calendar days of this policy's implementation. Agency policies shall include the responsibilities for LEOs to carry,

---

<sup>1</sup> See *DHS Commitment to Nondiscriminatory Law Enforcement and Screening Activities* and related updates: "DHS policy prohibits the consideration of race or ethnicity in investigation, screening, and enforcement activities in all but the most exceptional instances."... "These self-imposed limits, however, do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor." *Id.*

operate, maintain, and secure BWC equipment, including when to activate and deactivate the BWCs. Agency policies shall identify specialized or sensitive investigative techniques or equipment that may require different treatment under the BWC policy. Implementation of DHS and Agency BWC policies are contingent on the Agency's resource availability and the Agency's deployment plan.

2. Provisions in this policy are considered minimum standards that Agencies must meet. If Agencies choose to do so, Agency policy may exceed the minimum standards set in this DHS policy.
3. DHS Agencies will work with the DHS Management Directorate, Office of the Chief Financial Officer to assess resource requirements to fully implement BWC programs that comply with this policy.

#### B. Metrics

In collaboration with the Agencies, the Office of Strategy, Policy, and Plans will develop a limited set of standard metrics that shall be tracked by each Agency's BWC program.

#### C. Privacy Compliance and Record Keeping

Agencies shall ensure their BWC programs are in full compliance with DHS privacy policies, including Privacy Policy 047-01, and that all privacy compliance documentation has been completed before piloting or operational use of BWCs. Agencies shall ensure BWC data is addressed in their records retention schedule and institute procedures to efficiently respond to Privacy Act and Freedom of Information Act (FOIA) requests in accordance with federal law and any applicable Executive Orders.

#### D. Training

Agencies will ensure that DHS personnel who operate or support the authorized use of BWCs and BWC data have received all required training in the use of BWCs and in relevant policies and procedures. This training will occur prior to their authorization to use BWCs or access BWC data, and DHS personnel must complete all applicable refresher training to maintain authorization to use BWCs or access BWC data. Agencies shall document completion of such training. BWC training shall include, at a minimum:

1. BWC operation, maintenance, and care;
2. Correct handling, storage, use, and dissemination of BWC data;
3. Privacy compliance and proper privacy and FOIA policy procedures for redacting, sharing, and disclosing BWC data to the appropriate parties pursuant to DHS and Agency disclosure policies;

4. Required, optional, and non-permissible uses of BWCs;
5. Officer/agent and public safety considerations when wearing/operating BWCs;
6. The laws, regulations, or policies governing the use of BWCs, including updates on changes; and,
7. Civil rights and civil liberties considerations (in consultation with the Office for Civil Rights and Civil Liberties).

#### **IV. LEO Responsibilities**

- A. Activation and Deactivation: LEOs are responsible for activating and deactivating BWCs as directed in Agency policies.
- B. LEOs are responsible for carrying, operating, maintaining, and securing BWC equipment as directed in Agency policies.
- C. LEOs shall use only DHS or Agency issued and approved BWCs and shall use such devices in accordance with DHS policy. The use of personally owned BWCs or other video, audio, or digital recording devices to record official law enforcement activities is prohibited.
- D. LEOs shall not intentionally tamper with or dismantle a BWC, its hardware or software, or otherwise intentionally interfere with BWC capabilities.
- E. LEOs shall upload BWC data at the end of each shift or as soon as feasible thereafter and ensure any BWC data in the LEO's possession is correctly maintained, stored, used, and disseminated.
- F. LEOs shall advise individuals as soon as practicable that they are being recorded. If the LEO believes providing such notice interferes with the law enforcement encounter or LEO safety, then notice shall be given if/when operationally feasible.

#### **V. BWC Data**

- A. General Provisions on BWC Data
  1. BWC data shall only be accessed, downloaded, shared, and disclosed by authorized DHS personnel for authorized DHS purposes as specified in Agency policies.

2. Common authorized purposes where authorized personnel may review BWC data include, but are not limited to, the following instances:
  - To complete investigations and prepare related investigative reports;
  - To support discovery obligations in connection with criminal prosecutions;
  - Prior to testifying before a grand jury and any court related proceeding, or as otherwise needed in connection with civil, criminal, or administrative proceedings;
  - For training purposes (with personally identifiable information (PII) redacted or sufficiently sanitized);
  - To evaluate claims of misconduct or other policy violations, including violations of civil rights and civil liberties;
  - To conduct authorized compliance activities, including audits and oversight reviews; and,
  - In preparation for administrative investigations/interviews.
3. LEOs shall state in their reports whether BWC recorded data was viewed prior to completing the report. Unless otherwise prohibited by an Agency policy, authorized DHS BWC users may review all available BWC recorded data that is relevant to a law enforcement encounter prior to writing initial reports regarding the encounter.
4. Data Retention: DHS personnel shall not intentionally delete or modify BWC recorded data and shall only dispose of BWC recorded data as permitted by the Agency's National Archives and Records Administration (NARA) approved records schedule and in compliance with any relevant FOIA requests or litigation holds.
5. Data Handling and Storage: BWC data shall only be stored in authorized DHS data systems. DHS personnel shall not intentionally modify BWC data. However, per Agency policy, Agencies may create a new copy of the BWC data for purposes of redacting or sanitizing such data for privacy or confidentiality purposes for further disclosure to appropriate parties, while maintaining the original copy. Systems or platforms used to store BWC data will include appropriate access controls and be in compliance with DHS information security requirements. These systems will be audited regularly to ensure access and system activities are consistent with authorized activities.
6. Redaction of Privacy Sensitive and Operationally Sensitive Data: Agencies shall review BWC data to ensure PII, victim identity information, and law enforcement sensitive or other operationally sensitive information are appropriately redacted for BWC data that will be

further disclosed to appropriate parties, to include circumstances where that data is publicly released, while maintaining the original copy. BWC data systems will log the identity of individuals redacting, sanitizing, or otherwise modifying BWC data.

7. BWCs Buffer: DHS BWCs shall be configured to automatically record at least 30 seconds of video prior to the BWC's activation.
8. BWC and Biometrics: Use of any facial recognition biometrics is governed by federal laws and regulations, DHS privacy policy, and DHS policies and guidance specific to facial recognition biometrics. Use of facial recognition in conjunction with live video from BWCs will be postponed until Department policies related to facial recognition biometrics have been approved. However, still pictures derived from BWC video data that has been uploaded into a system of record, in compliance with applicable privacy requirements and protections, may be used to support authorized law enforcement activities.

B. Public Release of BWC Data

1. Requests for BWC data are subject to all applicable laws, regulations, and DHS and Agency policies, including but not limited to the FOIA and the Privacy Act of 1974.
2. Requests from the public (which includes individuals captured in BWC data), Congress, and the press shall be coordinated and processed according to each Agency's BWC policy, the Privacy Act of 1974, and the FOIA. In all cases, the LEO who recorded the data will be notified of the release of their data prior to release.
3. Expedited Public Release of BWC Data: Agencies shall develop protocols, in accordance with and subject to any applicable DHS Privacy protocols and policies, for expedited public release of BWC data following incidents involving serious bodily injury or deaths in custody. Agencies shall expeditiously review the data and approve for public release as soon as practical, subject to ensuring any data is redacted to protect the privacy rights of the persons depicted in the data, or other individuals' privacy implicated from such data, or to protect ongoing law enforcement operations. The LEO who recorded the data will be notified of the release of their data prior to release. Upon approval within the Agency, the Agency may immediately release the data with any necessary redactions.
  - Agencies will consult with the United States Attorney's Office in the responsible federal district prior to the expedited release of BWC data.

- If there are specific and compelling circumstances justifying an objection to public release that cannot be resolved by redaction or other means, Agencies may withhold release of the BWC data.
- Agencies shall notify the DHS Office of Public Affairs prior to external release of any BWC data that documents death or serious bodily injury.

## **VI. BWCs and Task Forces**

### **A. For law enforcement task forces led by DHS or a DHS Agency:**

1. The DHS Agency leading a task force shall establish agreements with participating law enforcement agencies to document the requirements for BWC use and data management, and ensure all task force participants are aware of and comply with the BWC requirements. Unless otherwise prohibited by another interagency agreement, DHS and Agency-led task forces will comply with this BWC policy. DHS and Agency-led task forces shall make clear in their written agreements that BWC data are deemed to be federal records owned by DHS and subject to federal retention and information access laws, regulations, policies, and procedures.
2. Task force officers (TFOs) who are assigned to DHS Agency-led task forces will comply with the lead Agency's BWC policy. If a TFO assigned to a DHS Agency-led task force does not have BWC equipment assigned to them by their parent agency, the lead DHS Agency shall, to the extent possible and depending on resource availability, make the Agency's BWC equipment and training available to the TFO.

### **B. For law enforcement task forces led by a non-DHS agency:**

1. DHS LEOs assigned to a task force that is not led by their Agency shall follow the BWC policies, procedures, and/or agreements established by the agency leading the task force.
2. Absent a signed agreement indicating use of another Agency's policy, DHS personnel assigned to a non-DHS task force shall follow their Agency's BWC policy.
3. BWC data recorded by a DHS LEO while on assignment to a task force led by a non-DHS agency are deemed to be federal records owned by the DHS LEO's parent Agency and subject to federal retention and information access laws, regulations, policies, and procedures.

4. For joint international operations or foreign law enforcement task forces, Agencies will ensure procedures for foreign TFOs and DHS LEOs are clearly documented. Absent such joint documentation, DHS personnel assigned to joint international operations or foreign law enforcement task forces shall follow their Agency's BWC policy.

## **VII. No Right of Action**

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

## **VIII. Definitions**

- A. **Body Worn Camera:** Audio/video/digital recording equipment combined into a single unit and typically worn on clothing or otherwise secured to a person, e.g., affixed to the outside of the carrier/tactical vest facing forward.
- B. **Law Enforcement Officer:** A position occupied by a DHS employee authorized by statute to enforce the laws of the United States, carry firearms, and make criminal arrests in the performance of their assigned duties.
- C. **Task Force Officer:** A law enforcement officer from a non-DHS law enforcement agency or office working jointly with law enforcement officers from other law enforcement agencies, including DHS.