United States Department of the Interior

FISH AND WILDLIFE SERVICE
Washington D.C. 20240

DIRECTOR'S ORDER NO.: 220

Subject: BODY-WORN CAMERAS

Sec. 1 What is the purpose of this Order?

a. This Order:

(1) Helps to ensure a consistent standard for when U.S. Fish and Wildlife Service (Service) Federal Wildlife Officers (FWO) can and cannot use Body-Worn Cameras (BWC) in the performance of their duties, and

(2) Governs the use and storage of the data BWCs collect.

b. This Order does not apply to digital or electronic media recordings from dash cameras, digital cameras, and closed-circuit television.

Sec. 2 What is the legal authority for this Order? The authority for this Order is the National Wildlife Refuge System Administration Act of 1966, as amended by the National Wildlife Refuge System Improvement Act of 1997 (16 U.S.C. 668dd-668ee).

Sec. 3 What are the fundamental requirements of this Order?

a. An FWO must wear a Service-issued body camera specifically assigned to him/her when performing law enforcement duties that involve, or could potentially involve, interactions with the public.

(1) The BWC must be one that the Service has purchased that can capture both video and audio data, and that automatically records the date and time of the recording with a minimum 30-second pre-event recording mode. The Chief, Division of Refuge Law Enforcement (DRLE) determines which BWCs the Service may purchase.

(2) The BWC must be compatible with the Incident Management Analysis and Reporting System (IMARS) and the Law Enforcement Management Information System (LEMIS).

(3) FWOs must not use non-Government-owned recording devices (e.g., personal digital cameras, smartphone cameras, etc.) for documenting law enforcement activities, including the documentation of evidence.

(4) FWOs must place the BWC on the body so that the lens is visible.

(5) If an FWO needs to use a BWC not assigned to him/her, the FWO must document that use.

b. The Headquarters Chief Technology Officer (CTO) approves storage solutions and authorizes procedures for downloading all BWC footage. The Regional CTOs will implement approved storage solutions and procedures and will manage the software maintenance needs for BWCs. Units will be returned to the manufacturer when there are hardware issues.

c, The Branch of Training, DRLE establishes the training requirements for using BWCs. FWOs must complete a DRLE-approved BWC training program before using a BWC during official duty. Approved training programs must be at least 1 hour and address:

(1) The operation of the BWC;

(2) Procedures for managing BWC footage; and

(3) The legal and ethical consequences for FWOs and the Service if an FWO makes unauthorized changes to the BWC or the data, individuals without a legal need to access the data view it, or an FWO releases data to the general public without authorization.

d. Law Enforcement Officers (LEO) who are supervisors, Federal Wildlife Zone Officers (FWZO), and Information Technology (IT) personnel who are designated to manage BWC footage must complete the following initial and annual followup training:

(1) Procedures for processing BWC footage for use as evidence,

(2) The required storage times for BWC footage, and

(3) How to safeguard BWC footage.

e. An FWO must assess the BWC prior to beginning his/her shift to determine if the camera has sufficient battery charge and available memory to meet the needs of the anticipated shift.

f. If an FWO determines that his/her BWC is nonfunctional, lost, or stolen, he/she must inform his/her FWZO and immediate supervisor. FWOs may continue to perform their law enforcement duties without the BWC when it’s nonfunctional and a replacement is not available.

(1) The FWO must document the BWC's damage or malfunction and provide the documentation to his/her supervisor and FWZO.

(2) If a BWC is lost or stolen, the FWO must report the loss or theft using the Serious Incident Notification Procedures policy (054 FW 1).

g. FWOs must conform with Memorandum LE-9, "Consensual Monitoring," dated 02/02/2007, when recording audio conversations in situations where they do not identify themselves as Federal LEOs or when they are not readily identifiable as Federal LEOs (i.e., not in uniform).

Sec. 4 When must an FWO activate a BWC?

a. An FWO must activate the BWC when any of the following occur:

(1) Interactions that give the FWO reasonable suspicion that there has been or may be a violation(s) of law(s)or regulation(s);

(2) Motor vehicle stops, which include vessels, all-terrain vehicles, utility vehicles, snow machines, etc.;

(3) Interactions with the public where the FWO perceives there may be hostility toward the FWO or others;

(4) During searches, seizures, and executions of warrants;

(5) When the FWO believes there is the need for supporting documentation of law enforcement activity;

(6) Prisoner transport if a vehicle camera is not available;

(7) When interviewing victims and witnesses of accidents (e.g., automotive, boating, hunting-related, etc.); and

(8) When the FWO determines there is the potential need for supporting documentation (e.g., transporting or transferring evidence or currency).

b. When feasible, an FWO must inform law enforcement personnel, emergency service personnel, and Service employees when the BWC is actively recording.

c. An FWO may only terminate the BWC's recording when he/she determines the event is over or as this guidance otherwise authorizes.

d. Even if an FWO does not believe a law enforcement event is over, he/she may temporarily deactivate or terminate the recording:

(1) When the FWO is speaking to confidential informants or undercover law enforcement, or when discussing law enforcement tactics or procedures; and

(2) During periods of time when there is no interaction with the public and the FWO is waiting for the incident to progress (e.g., waiting for a tow truck or waiting for a boat to return to a ramp, etc.).

e. FWOs must follow these procedures for temporary or premature termination of a recording:

(1) To address the deactiviation/ termination of the electronic recording, the FWO should speak into the microphone of the BWC and explain the intent and reason(s) for the temporary deactivation or the termination of the recording.

(2) When the FWO reactivates the body camera, he/she should state that he/she has restarted the recording.

(3) The FWO must document the reason(s) in the patrol log or incident report for temporary or premature termination of a recording.

Sec. 5 When must an FWO NOT activate a BWC?

a. An FWO must not activate the BWC in bathrooms or locker rooms unless he/she is doing so to pursue a law enforcement investigation, a warrant, an arrest, or in exigent circumstances.

b. In locations where there is a reasonable expectation of privacy (e.g., residence, place of worship), the FWO must ask permission before recording with the BWC unless he/she cannot ask permission first because it would hamper the law enforcement investigation, warrant, arrest, or it is an exigent circumstance.

c. An FWO must not record non-official activity. For example, he/she must not record family members or Government employees not involved in a law enforcement investigation, except for training purposes or to test the camera.

d. An FWO must not covertly record the general public at large. Absent a connection to an investigation, law enforcement activity, or a citizen request for assistance, FWOs are prohibited from recording First Amendment demonstrations.

e. An FWO must not set up the BWC to record while he/she is not attending to it, except under circumstances where a citizen would not normally have a reasonable expectation of privacy, such as in the backseat of a patrol vehicle.

f. If an FWO does not activate the BWC, or the recording was interrupted or was terminated for reasons listed previously, he/she must explain the reason(s) in the patrol log or incident report.

Sec. 6 When may an FWO delay activating a BWC or discontinue its use?

a. FWOs may delay the activation or discontinue the use of their BWCs when they believe that activating them would:

(1) Endanger the FWO, another LEO, a suspect, or the general public; or

(2) Interfere with their response in a dynamic situation.

b. When an FWO delays activating the BWC, he/she must explain the reason(s) for delayed activation in the patrol log or the incident report.

Sec. 7 What are the exceptions to wearing a BWC? FWOs do not have to wear their BWCs when:

a. Wearing Class A uniforms, performing a ceremony for the public, or performing duties that do not involve interacting with the public in a law enforcement manner;

b. In court or in any other judicial meeting (e.g., grand jury, depositions, etc.);

c. In training, conferences, travel status, and during law enforcement exercises;

d. The FWO's FWZO or Regional Chief, DRLE, authorizes him/her to perform his/her duties without wearing the BWC; and

e. Assigned to a position (e.g., administrative duties) or a location (e.g., Regional office) where they are not tasked with direct law enforcement duties.

Sec. 8 What are the standard operating procedures for storing BWC data?

a. Prior to beginning the next shift, an FWO must download BWC footage to a storage repository in its entirety. For those stations with connectivity issues, refer to section 8(d). If an FWO cannot download BWC footage due to remote circumstances (i.e., details, working in areas with no internet or that have electricity access issues), he/she must download the footage as soon as he/she is able to so.

b. All data, including video, audio, and digital images, must be stored in a Service-provided and internet-accessible repository (server) that is designed for the storage of sensitive law enforcement data.

(1) FWOs must not alter or delete BWC data.

(2) FWOs must not store BWC data on a desktop computer or a laptop that is not secured in evidence storage.

c. The minimum connection speed required for connecting to the central repository over the network is T1 or 1.544 Megabits per second (Mbps).

d. If a Service-provided, central repository is not accessible due to connectivity limits at the refuge level, the FWO must store BWC data using practices that adhere to Service (445 FW 3, Evidence) and Departmental (446 DM 7, Evidence Handling and Storage) policies for the proper storage and handling of evidence. If the data is stored on an external hard drive, the basic requirements include the following:

(1) The hard drive must be a Solid State External Hard Drive (SSD).

(2) The data must be encrypted with the Advanced Encryption Standard (AES) 256.

(3) The SSD must be stored in a secure, climate controlled environment, and in a shock resistant case.

(4) Video stored in this manner must contain a unique identifier in the file name to correspond with the Law Enforcement Management Information System (LEMIS) incident number.

(5) If there's an SSD failure, the Service must use a data recovery vendor that the Information Resources and Technology Management (IRTM) program approves. If data is lost that we are required to permanently retain, the FWO or other law enforcement personnel must contact the Service Records Officer within 48 hours of discovery. The Service Records Officer must prepare a records loss report and send it to National Archives and Records Administration (NARA).

e. If an event generates a LEMIS incident report, all video, audio, and digital images associated with that event must be stored as an attachment to the LEMIS incident report. If a station's limited connectivity makes uploading the video to LEMIS impractical, the Regional Chief, DRLE, may approve storing the digital evidence as we describe in subsections 8(a) - (e) only. Video stored in this manner must contain a unique identifier in the file name to correspond with the LEMIS incident number. The LEMIS incident report for the event must indicate that BWC footage exists.

f. A non-incident recording is one that does not generate a LEMIS report. The BWC data for such incidents must be stored in the Service-provided and IRTM-approved non-incident central repository allocated for each FWO. If connectivity issues do not allow for access to the non-incident central repository, the FWO must use an SSD specifically designated to store non-incident data. The SSD must meet the requirements for storage and handling that we describe in subsection 8(e). BWC data obtained from routine surveillance (i.e., data not associated with an incident) will be destroyed as we describe in section 9.

g. No original video, audio, or photographic evidence may be permanently altered in any way prior to deletion. The Chief, DRLE may authorize temporary alterations to copies of original evidence.

h. FWOs may activate the BWC for testing and training, but must follow standard operating procedures for retaining those captured videos.

Sec. 9 What are the standard operating procedures for retaining and destroying recordings?

a. At the field level, only FWZOs are authorized to destroy BWC data. An FWZO may only destroy BWC data for his/her areas of responsibility when appropriate.

(1) FWZOs may use IRTM-approved BWC system software with programmable deletion and retention protocols. Data deletion cannot occur if the Service's records classification number is frozen. The FWZO should check with the Service Records Officer for approval prior to deleting data.

(2) When FWZOs use this software, they are responsible for following the retention and deletion protocols we describe in this policy.

b. The storage of BWC data associated with a LEMIS report must comply with USFWS Disposition Manual, Enforcement, ENFR-110 Law Enforcement Management Information System (LEMIS) (N1-022-05-01/63). The Disposition Manual states that the Service must retain the BWC data with the LEMIS report, and it can only be deleted 20 years after the case is closed.

c. FWZOs must destroy BWC data not associated with criminal investigations after 30 days in accordance with the NARA General Records Schedule disposition authority (DAA-0048-2015-0002-0001) addressing routine surveillance recordings, which follows:

"These recordings are produced and maintained in the course of routine security measures for facilities and public lands administrated by DOI and are characterized by being necessary for day-to-day operations but not suitable for long-term preservation. These surveillance recordings are of a non-evidentiary value and will be automatically destroyed after 30 days. In the event that a recording is identified as relevant to a particular legal or investigative case file, the recording will be included as part of the case file and retained according to the approved records disposition schedule for that case file."

d. FWZOs must destroy BWC data obtained during training and testing within 30 days, except when the Chief, DRLE approves its retention.

e. FWZOs must treat unintended recordings in the same manner as BWC data not associated with criminal investigations or that was produced for training or testing.

f. BWC data documenting physical altercations or injuries must be retained with its associated LEMIS report and follow the retention schedule described in subsection 9(b).

g. When the Service is challenged by the Court, we must treat the BWC data as part of the litigation case file and the data retention must comply with INFO-410 Litigation Case Files (NC1-22-78-1/59). Following is an excerpt:

> *"[A]ll other substantive materials concerning any lawsuit in which the Service is a participant. The responsibility for maintenance of record material in this series rests with the Department of the Interior. Retention: TEMPORARY. Destroy 5 years after all parties have exhausted all apparent legal recourse."*

h. All originals and copies of video, audio, and image data that a BWC gathers are the sole property of the U.S. Government and are subject to the protections and guarantees of the Freedom of Information Act (FOIA), the Privacy Act, the Federal Records Act, and all other applicable laws and regulations.

Sec. 10 What are the standard operating procedures and limitations for accessing BWC data?

a. Network speeds: When accessing video data directly from the central repository, the minimum network speeds needed to avoid disruptions in viewing the video are noted in the table below.

Resolution	Recommended Minimum Speed
480p	3 Megabits per second
720p	6 Megabits per second
1080p	10 Megabits per second

b. Service employee access:

(1) The Chief, DRLE has access to all BWC data stored in approved repositories and LEMIS.

(2) The Regional Chiefs, DRLE have access to all BWC data obtained in their Regions.

(3) FWZOs have access to the BWC data for the FWOs for whom they are responsible.

(4) The FWOs may review their own BWC footage to help them prepare accurate reports or to refresh their memories before making statements about recorded incidents.

(5) FWZOs/Commissioned LEO Supervisors may review BWC footage during the investigation of complaints and to identify BWC footage appropriate for training or instructional use. A non-commissioned supervisor may work through the FWZO or Regional Chief, DRLE if he/she needs to view footage.

c. Other official access:

(1) We can give the U.S. Attorney's office, States' Attorney's offices, the Service Professional Responsibility Unit (PRU), and other law enforcement agencies temporary and restricted access to case-specific BWC data stored in the repository, as needed. The FWZO approves such requests on a case-by-case basis.

(2) We grant this access using an encrypted Universal Serial Bus (USB) drive. The USB drive allows us to handle the data in a way that maintains a chain of custody as required by Service and Departmental policy (445 FW 3 and 446 DM 7).

d. Public/media access: The public and media may only request video or audio recordings from BWCs under FOIA (see 203 FW 1). If release of BWC video or audio is appropriate, the Service FOIA Officer will work with the Chief, DRLE and the Chief, National Wildlife Refuge System (NWRS), before approving any releases.

(1) The Chief, NWRS must consult with the Department's Director, Office of Law Enforcement and Security (OLES), before the Service FOIA Officer may release any BWC data to the general public.

(2) The Director, OLES will review and provide a written response within 72 hours of being sent FOIA requests to release BWC data.

(3) BWC data must not be released based on a FOIA request until all investigations by the Service and all other law enforcement agencies associated with the data are complete, unless the Director, OLES and the Chief, NWRS approve it.

(4) If data associated with a PRU investigation is requested through FOIA, it cannot be released until the PRU investigation is complete.

e. Auditing storage and access: FWZOs must conduct random, semi-annual audits of stored BWC data within their zones to ensure the equipment is operational and that FWOs are complying with policy and procedures.

(1) The audit must include at least five videos within the LEMIS system and five videos involving law enforcement activity that did not generate LEMIS reports.

(2) If data is stored on an external SSD, the FWZO must acquire and transfer the data when the SSD is 90 percent full or semi-annually when performing audits, whichever is shorter.

Sec. 11 What are the standard operating procedures for altering BWC data?

a. Original data must not be edited or altered. Only the Chief, DRLE may approve the temporary alteration of copies of BWC data.

b. The Chief, DRLE may approve temporary changes to copies of BWC data only in the following situations:

(1) To ensure constitutionally or statutorily protected privacy rights and interests;

(2) To protect personally identifiable information;

(3) To protect the identity of an undercover LEO, confidential informant, criminal witness, or juvenile; or

(4) When a video contains nude images or images that are graphic in nature so the images should be pixilated before they are released.

c. Temporary changes may only include pixilation and muting the audio.

(1) FWOs and FWZOs must not reduce the length of a video.

(2) FWOs and FWZOs must only use Service-approved software for pixilation, muting audio, or compression. IRTM determines which pixilation, muting, and compression software may be used.

Sec. 12 What is the standard operating procedure for BWC data if an FWO is involved in a shooting? An FWO must immediately secure the BWC as evidence after securing the crime scene. He/she should only surrender the BWC to the FWZO; the Regional Chief, DRLE; a designated representative of the PRU; or as otherwise directed by the Chief, DRLE. The FWO must not surrender the BWC to any other party unless specifically directed by the Chief, DRLE.

Sec. 13 When is this Order effective? This Order will be effective immediately. It remains in effect until we incorporate it into the U.S. Fish and Wildlife Service Manual, or until we amend, extend, supersede, or revoke it, whichever comes first. If we do not amend, extend, supersede, or revoke it, the provisions of this Order will terminate 18 months from date of signature.

/sgd/ Margaret E. Everson
PRINCIPAL DEPUTY DIRECTOR

Date: May 6, 2019