BRIEFING STATEMENT

PREPARED FOR: NWRS LEADERSHIP TEAM

DATE: May 28, 2018

TITLE: Status of Director's Order on Body Worn Camera (BWC)

ISSUE: The Department of the Interior, Office of Law Enforcement and Security, requires all Bureau law enforcement programs to have National policy regulating the use of body worn cameras (BWC) and the management of BWC data.

BACKGROUND:

Headquarters has been actively working with Regional law enforcement leadership, Federal Wildlife Officers, Information Technology (IT), the Solicitor's Office, and the Professional Responsibility Unit to develop National policy on BWC for the past two years. (b) (5) DPP [redacted]

STATUS/KEY POINTS:

- (b) (5) DPP [redacted]

ACTIONS: Informational

PREPARED BY: Richard A. Johnston, Chief – Division of Refuge Law Enforcement

DIRECTOR'S ORDER NO.: (Leave this blank. PDM will assign the number.)

Subject: BODY-WORN CAMERA

Sec. 1 What is the purpose of this Order? The purpose of this order is 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 governs the use and storage of the data BWCs collect. This memorandum does not apply to digital or electronic media recordings from dashboard cameras, digital cameras, and closed-circuit television.

Sec. 2 What is the legal authority for this Order?

a. (b) (5) DPP [redacted]

b. 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) 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.

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

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

b. A training manager will establish the training requirements for using BWCs;

c. FWOs must complete a DRLE-approved BWC training program before using a BWC during official duty. An approved training program must include at least one hour addressing:

(1) The operation of the BWC;

(2) Procedures for managing BWC footage

(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; and an FWO releases data to the general public without authorization

d. LEO Supervisors, Federal Wildlife Zone Officers (FWZO) and IT personnel who are designated to manage BWC footage must complete the following initial and annual follow-up 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 at the beginning of his/her shift to determine if the camera has sufficient battery charge and available memory to meet the needs of the anticipated shift.

(1) 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; and

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

f. 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 law enforcement officers, or when they are not readily identifiable as federal law enforcement officers (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 indicate reasonable suspicion of a violation(s) of law(s)or regulation(s);

(2) Motor vehicle stops, including 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. If an FWO does not believe a law enforcement event is over, he/she may temporarily deactivate or terminate the recording in the following circumstances:

(1) The FWO may temporarily deactivate the BWC when speaking to confidential informants or undercover law enforcement, or when discussing law enforcement tactics or procedures;

(2) The FWO may temporarily deactivate the BWC 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); and

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

i. To document the deactiviation/ termination, the FWO may speak into the microphone of the BWC the intent and

reason(s) for the temporary deactivation or the termination of the recording.

ii. When the FWO reactivates the body camera, they may state they have restarted the recording.

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

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

c. An FWO must not record non-official activity. For example, he/she must not record family members and/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 nexus to an investigation, law enforcement activity, or a citizen request for assistance, an FWO is prohibited from recording first amendment demonstrations; or

e. Recording while the BWC is not attended by a uniformed LEO is prohibited, 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 for reasons listed previously, he/she must explain the reason(s) in the patrol log or incident report.

Sec. 6 When must a FWO delay activating a BWC?

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

(1) Endanger the FWO, another law enforcement officer, 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 BWC 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; or

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 their next shift, an FWO must download BWC footage to a storage repository in its entirety. For those stations with connectivity issues, refer to Sec. 9(c). In situations where a FWO is not able to download BWC footage due to remote circumstances (i.e. details, working in areas with no internet/ electricity access), he/she is to download the footage as soon as they are able to;

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. 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 a shock resistance 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; and

(5) If there's an SSD failure, the Service must use a data recovery vendor that has been approved by the Information Resources and Technology Management (IRTM) program. For permanent retention items, upon discovery, the FWS Records Officer must be contacted within 48 hours and a records loss report must be prepared by the FWS Records Officer and reported to National Archives and Records Administration (NARA).

d. 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 has limited connectivity and uploading all video to LEMIS is not practical, the Regional LE Chief may approve the digital evidence to be stored as identified in Sec. 9 (a) and (b) only. Video stored in this manner must contain a unique identifier in the file name to correspond with the LEMIS incident number.

e. For recordings that do not generate a LEMIS report, the BWC data must be stored in the Service-provided and IRTM-approved non-incident central repository allocated for each FWO. If refuge level internet connectivity limits do not allow for access to the non-incident central repository, the FWO must use an SSD specifically designated to store non-incident data, and that SSD still must meet all the requirements for storage and handling described for data storage on SSDs for incidents identified in Sec. 9 (b).
(6) The retention of BWC data obtained from routine surveillance (i.e. data not associated with an incident) will be destroyed following the time constraints described in Sec. 10 (c).

f. 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;

g. 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 Bureau records classification number is frozen. The program lead should check with the FWS Records Officer for approval prior to deletion.

(2) When FWZOs use this software, they are responsible for ensuring that retention and deletion protocols in this guidance are followed.

b. 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) which states the BWC data must be retained with the LEMIS report and will be deleted 20 years after the case is closed;

c. FWZOs must destroy BWC data not associated with criminal investigations, training, or testing after 30 days in accordance with the National Archives and Records Administration 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 (accidental) recordings in the same manner as BWC data not associated with criminal investigations, training, or testing;

f. BWC data documenting physical altercations or injuries must be retained with its associated LEMIS report and must follow the retention schedule we

describe in Sec. 10 (b) above.

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 all 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 for accessing BWC data?

a. Service employee access:

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

(2) The DRLE Regional Chiefs 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 FWO may review BWC footage to aid them in preparing accurate reports or to refresh their memories before making a statement about a recorded incident.

(5) The FWZO/ Uniformed LEO Supervisor may review BWC footage during the investigation of complaints and to identify BWC footage appropriate for training or instructional use.

b. Other official access:

(1) We can give the U.S. Attorney's office, States' Attorney's office, 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.

(2) We grant this access using an encrypted Universal Serial Bus (USB) drive. The FWZO may approve this request on a case by case basis.

The USB drive will maintain a chain of custody outlined in the Service 445 FW 3 Evidence and Departmental 446 DM 7 Evidence Handling and Storage policies.

c. Public/media access: All public and media requests for video or audio recordings must follow the FOIA guidelines. Service FOIA officers direct FOIA requests related to BWC data to the Chief, DRLE, for review. The Chief, DRLE, gives his/her recommendation to the Chief, National Wildlife Refuge System (NWRS), for approval or disapproval.

(1) The Chief, NWRS must consult with the Department of the Interior Director, Office of Law Enforcement and Security (OLES) before releasing any BWC data to the general public.

(2) The Director, OLES must review all FOIA requests to release BWC data before the Chief, NWRS may release it.

(3) BWC data must not be released based on a FOIA request until all investigations by the U.S. Fish and Wildlife Service and all other law enforcement agencies associated with the data is complete, unless the Chief, NWRS approves it and only after he/she consults with the Director, OLES.

(4) Data associated with a PRU investigation, based on a FOIA request, will not be released until the PRU investigation is complete.

d. 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 stored data when the SSD is 90 percent full, or semi-annual, whichever is shorter, when performing audits.

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

a. No one may permanently alter BWC data. Only the Chief, DRLE may approve the temporary alteration of copies of BWC data. Original data must not be edited or altered;

b. The Chief, DRLE may approve temporary changes to BWC data stored in the repository or copied to electronic storage 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 law enforcement officer, confidential informant, criminal witness, juvenile; or

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

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

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

(2) FWOs and FWZOs must only use Service-approved software for pixilation, muting of audio, or compression. The Service Associate Chief Information Officer – IRTM determines which pixilation, muting, and compression software is authorized

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 should 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 Fish and Wildlife Service Manual, or until we amend, supersede, or revoke it, whichever comes first. If we do not amend, supersede, or revoke it, the provisions of this Order will terminate on (date).

Director

Date: