

U.S. MARSHALS Body Worn Camera Program

TFO BWC MOU ADDENDUM Appendix A

The following is controlling guidance for situations that may affect a Task Force partner agency regarding the TFO (Task Force Officer) BWC (Body Worn Camera) MOU (Memorandum of Understanding) Addendum. This guidance is issued by the United States Marshals Service (USMS) Body Worn Camera Program (BWCP) and USMS Office of General Counsel(OGC):

- Review Boards/Other Public Dissemination: If an agency is under a consent decree or otherwise required by statute, law, or agreement to disclose BWC footage to a review board, that entity and their access to the agency BWC and the qualifying events or incidents that are the subject of the agreement will be described in a letterhead memo that the USMS will keep in the BWC MOU tracking system. The memo should include the timeline for that board to receive the footage, if their access to an agency BWC Video Retention System is direct or indirect, and whether the review board has independent/unilateral public disclosure authority. This information will assist the USMS OGC in determining what timeline they may be under to perform agency review if a qualifying incident occurs where TFO and/or USMS BWC footage has been recorded.
- State Law/Agency Policies: If state law or qualifying agency policy requires recording outside the parameters of USMS TFO BWC MOU Addendum, the agency will provide that information and a copy of the policy to the USMS BWCP. The recordings of post-arrest events that are outside TFO enforcement action, i.e., medical facilities, prisoner transport, should be separated, if possible, by deactivation of the TFO BWC when the arrest scene is concluded and secure; and reactivation when the officer is operating under his agency policy alone for a non-TFO agency responsibility. When separate recording(s) are possible, the USMS will receive only the enforcement BWC recording. If deactivation and reactivation are not feasible or are not permitted by state law or parent agency policy, the entire recording will be shared with USMS with the understanding that USMS will, if necessary, redact the entire portion of any recording that shows the TFO performing an agency duty where he is not operating under the USMS Task Force (TF) MOU parameters for enforcement actions.
- Short term operations: Any partner TF agency not covered by an existing executed USMS TFO BWC MOU Addendum and any non-partner state, local, federal, or tribal agency are authorized to utilize their BWC during a USMS short term operation or USMS led national initiative after agreeing to share any BWC footage obtained during the operation with the USMS upon request. Any BWC footage of a critical incident such as an Officer Involved Shooting or other use of force leading to death will be shared as soon as possible after the incident. Other footage will only be requested if the USMS has a mission-related requirement that can only be supported by receipt of the BWC recording from the BWC agency. Short term operations are defined for the purpose of this Appendix as USMS Enforcement related operations where a Special Deputization is issued or mass Special Deputizations are performed. These include, but are not limited to, Operation Washout, Operation Triple Beam, USMS National Initiatives for Enforcement and any DOJ directed initiative that is enforcement oriented and led by the USMS.

Rev. 08/24/22

Addendum to Fugitive Task Force Memorandum of Understanding RE: Body-Worn Camera Use by Task Force Officers

This Addendum supplements the current Memorandum of Understanding (MOU) between the United States Marshals Service (USMS) and the

(Hereinafter referred to as "Partner Agency" or "TFO parent agency")

Pursuant to the "U.S. Marshals – Body Worn Camera Interim Policy," dated May 17, 2022, and any successor USMS Body Worn Camera Policy Directive (hereinafter referred to as "USMS Policy"), the above-named Partner Agency has advised the USMS that it will require its Specially Deputized Task Force Officers (TFO) assigned to the USMS Task Force to use body worn cameras (BWCs). This Addendum governs that use.

The parties hereby agree to the following:

- I. The Partner Agency and their TFOs will be advised of and adhere to the USMS Policy, USMS's Standard Operating Procedures for Body-Worn Camera Program for Task Force Officers, and other applicable federal and USMS policies, procedures, regulations, and laws.
- II. The Partner Agency confirms that prior to executing this agreement, it has provided to the USMS details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFOs' use of BWCs, including any retention policies, and training and access procedures.
- III. TFOs will follow the provisions set forth in this agreement for use of BWCs. Absent an express conflict with state law or partner agency policy, the provisions in this agreement control TFO use of parent-agency issued BWCs on USMS task force operations.
- IV. Use of BWCs During USMS Task Force Operations:
 - A. TFOs may use only Partner Agency-issued and Partner Agency-owned BWCs.
 - B. TFOs will be allowed to wear and activate their BWCs for the purposes of recording their actions during USMS Task Force operations only during:
 - 1. A planned attempt to serve an arrest warrant or other planned arrest; or,
 - 2. The execution of a search warrant.

- a. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.
- C. TFOs are authorized to activate their BWCs upon approaching a subject or premises and must deactivate their BWCs when the scene is secured as determined by the USMS Task Force Supervisor or Team Leader on the scene.
 - 1. For purposes of this agreement, the term "secured" means the scene is safe and under law enforcement control.
 - In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement officer.
- D. Unless parent agency BWC policy and/or state law conflicts, TFOs are authorized to wear and activate recording equipment, in accordance with USMS Policy, anywhere they are authorized to operate under the scope of their USMS TFO deputization (to include on enforcement actions crossing jurisdictional boundaries). Where parent agency BWC policy and/or state law conflicts with the USMS activation and deactivation parameters, TFO's will follow the provisions in Appendix A that identify how to properly mark sections of a recording to ensure that the USMS task force operation captured on footage is easily identifiable. This will prevent the ingestion of non-task force related footage into the USMS video retention solution and allow USMS to promptly respond to requests for BWC footage.
- E. In the event a TFOs' BWC is not working or is inoperable due to a technical problem or cannot be used due to physical damage, the TFO may participate in the operation without using a BWC if that continued participation is consistent with the Partner Agency policy.
- F. Even when BWC use would be permissible in the circumstances set forth in Section IV, subsection B, above, TFOs are prohibited from recording:
 - Undercover or covert personnel and locations;
 - 2. Confidential informants or confidential sources;
 - 3. On-scene witness interviews prior to or after the operation; or
 - 4. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel prior to or after the operation.
- G. Even when BWC use would be permissible in the circumstances set forth above in Section IV, subsection B, TFOs are prohibited from activating their BWC if, as determined by the USMS, the TFO is:

Page 2 of 6

- 1. Using specialized or sensitive investigative techniques;
- 2. Operating as part of a highly specialized or sensitive operation or group;
- 3. Operating in a sensitive area; or
- Working in an undercover or covert status on behalf of the USMS Task Force or the USMS itself
- H. Even when BWC use would be permissible in the circumstances set forth above in Section IV, subsection B, subject to the discretion of the USMS, TFOs generally shall not use BWCs to record any activities related to investigations involving:
 - Public Corruption;
 - 2. Medical Facilities;
 - 3. National Security (including international and domestic terrorism investigations or cases involving classified information); or
 - 4. Other sensitive investigations as determined by the USMS.

V. Partner Agency Internal Controls:

- A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recording(s), and associated metadata, from TFO BWCs made while the TFO is working under federal authority, including when executing state and local warrants adopted by the USMS.
- B. The Partner Agency will provide and maintain central points-of-contact (POC), at a minimum two POCs, a primary and secondary, for the USMS on BWC matters. The Partner Agency will notify the USMS of any change to the POCs.
- C. The Partner Agency will notify the USMS of any change in state or local law or policy that will modify how TFOs must use BWCs and handle recordings.
- D. The Partner Agency will notify the USMS prior to making any change in agency policy that will affect the MOU Addendum or the storage, transfer, or redaction of TFO BWC recordings.
- E. The Partner Agency will provide specifications to USMS personnel on the BWC capabilities and operation.
- F. If applicable, the Partner Agency will restrict access to any TFO BWC GPS and/or livestream capability as required by the USMS.
- VI. Handling of TFO BWC Recordings Made During USMS Task Force Operations:
 - A. After a Task Force Operation, the TFO will upload any BWC footage into the Partner Agency's video retention system (VRS) and share a copy of that footage

Page 3 of 6

with the USMS. All copies of TFO BWC recordings made during federal Task Force Operations and shared with the USMS via the USMS VRS shall be deemed federal records of the DOJ/USMS pursuant to the Presidential and Federal Records Act Amendments of 2014 (Pub. L. No. 113-187, enacted November 26, 2014), and subject to federal disclosure rules and regulations, including the Freedom of Information Act (FOIA, 5 U.S.C. § 552) and Privacy Act of 1974. The original footage that remains in the custody of the Partner Agency shall not be disseminated by the TFO or TFO Partner Agency without advance written notification to the USMS of the intention to do so as soon as practicable

- B. The Partner Agency will provide full, unredacted, duplicate copies of TFO BWC recordings to the USMS for all activations that record data of USMS Task Force- related Operations. The existence of TFO BWC recordings relating to a USMS Task Force Operation must be recorded in the USMS authorized record system. Additionally, an unredacted copy of any recording to be released by the TFO Partner Agency shall be provided to the USMS prior to said release.
- C. The Partner Agency is authorized to use the original TFO BWC recordings for internal review of its personnel consistent with the Partner Agency's policies and procedures but may not disseminate the BWC recording outside the Partner Agency or publicly release the footage without advance written notification to the USMS. The Partner Agency's original TFO BWC recording is subject to the relevant state open records laws and state retention requirements.
- D. The Partner Agency will notify the USMS immediately of any unauthorized access to TFO BWC recordings discovered by the Partner Agency. The Partner Agency will cooperate fully with the USMS in the investigation of any unauthorized access to or disclosure of TFO BWC recordings, including providing the USMS with the name(s) of any Partner Agency personnel determined by the Partner Agency to be involved in unauthorized access, copying, or disclosure.
- E. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information. The premature disclosure of these recordings could reasonably be expected to interfere with enforcement proceedings. TFO BWC recordings may be potential evidence in a federal investigation subject to applicable federal laws, rules, and policy concerning disclosure or dissemination and therefore are deemed privileged, absent appropriate redaction prior to disclosure or dissemination. Further, BWC recordings may be entirely exempt from public release or other disclosure or dissemination under applicable federal and state laws, rules, and policy.
- F. If a TFO BWC recording involves a "reportable incident," as defined below, or involves another time-sensitive or urgent situation, the Partner Agency will provide the USMS access to copies on an expedited basis, including during non-business

hours.

- 1. For purposes of this provision, "reportable incident" means:
 - a. shooting incident;
 - any incident which involves serious bodily injury, death, or where any enforcement action by USMS personnel resulted in the use of force or deadly force;
 - physical assault or attempted physical assault on a Law Enforcement Officer; and
 - d. intentional damage to any facility, conveyance, or other property owned by USMS.
- G. The Partner Agency will provide witnesses, as needed, to authenticate TFO recordings in litigation.
- H. The Partner Agency will inform the USMS of the length of time TFO BWC recordings will be retained by the Partner Agency before deletion.
- I. The Partner Agency will notify the USMS in writing as soon as possible regarding any request or demand for release or disclosure of TFO BWC recordings. In all circumstances, TFO BWC recordings may only be disseminated in accordance with the requirements contained within this MOU addendum.
- J. Expedited Public Release: If TFO BWC recording(s) depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFOs' Partner Agency shall notify the USMS as early as possible if it desires to publicly release the recording(s). Following the notification, the TFO's Partner Agency may immediately release the recording(s) with any redactions as appropriate, giving as much advance notice as possible to the USMS as to the time and manner of its release. The USMS will expeditiously review the recording(s) as soon as practical.

	(b)(7)(E)		

K. An USMS enforcement action or incident may require additional support from law enforcement officers with the Partner Agency. In the event those assisting law enforcement officers have BWCs, any captured video from Page 5 of 6 those cameras will be made available by the Partner Agency to the USMS upon request.

- VII. The USMS will ensure that all USMS Task Force partner agencies are informed of which other partner agencies, if any, mandate BWC use by their respective TFOs and are authorized to have their TFOs wear BWCs on the USMS Task Force.
- VIII. If the Partner Agency fails to comply with any part of this Addendum, the relationship established under the Task Force Memorandum of Understanding may be immediately terminated.



From: (b)(6); (b)(7)(C); (b)(7)(F) (USMS)

Sent: Mon, 25 Nov 2019 21:23:20 +0000

 To:
 (USMS)

 Cc:
 USMS)

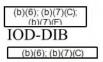
 Subject:
 Fwd: BWC Checklist

Attachments: BWC Checklist 11.25.19.docx, ATT00001.htm

(b)(6);

Please review the attached. This is the final draft with appropriate format, grammar and wordsmithing edits. Let us know if any additional edits are needed.

Once approved, I will share with the Pilot City Group.



Begin forwarded message:

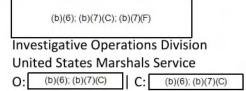


Subject: BWC Checklist

Hi Chief,

Please see attached for the checklist with all revisions we discussed today. Let us know if there are any other additional edits you'd like to make!

Thank you,



Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege

(b)(6); (b)(7)(C); (USMS) From: Sent: Wed, 1 Apr 2020 19:09:56 +0000 (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (USMS); (b)(6); (USMS) To: (b)(6); (b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); (USMS); (USMS) (b)(6); (b)(7)(C); (b)(7)(F) Cc: (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); USMS); (USMS) (b)(6); (b)(7)(C); **RE: BWC Documents** Subject: Attachments: Categories-Tags-4x6.pdf, USMS VRS Governance_Final.docx, USMS VRS Orientation Guide_Final.docx

(b)(6); (b)(7)(C); (b)(7)(F)

ALCON,

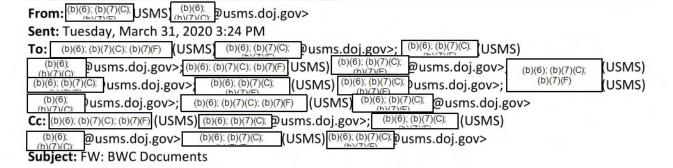
Attached are the final versions of the User Guide (what will accompany the shorter walk through doc provided) as well as the Governance guide (more relevant to us at the Oversight/HQ level for how we are using the system). I have also attached the 4x6 categories/tags PDF mentioned in my previous email.

(b)(6); (b)(7)(C);

Reviewed your two attachments and believe they convey the technically correct information and appropriate steps. It matches up with the UG well!

V/R,

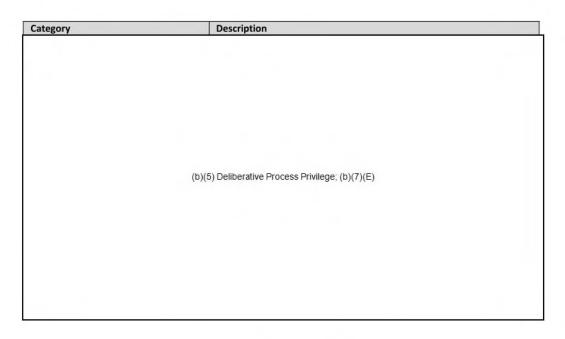


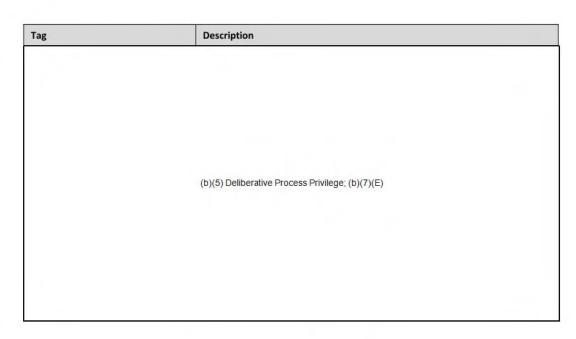


All;

Please review the attached and give final feedback on content accuracy. We are trying to finalize these docs and get them out to the field this week. Looking for feedback specifically on the reporting in JDIS comment in the Axon Walk-thru doc.

the Walk-thru doc was pretty much cut and paste from the full User Guide. However, we did make some edits and have some comments. Please ensure this is technically accurate as a minimal step by step walk-thru. Will the Appendix 2 charts of Categories and Tags be available as a separate doc from the User Guide? (b)(6); (b)(7)(C); (b)(7)(F) please ensure that our 1 page Quick Reference for the pilot program conveys the most important points appropriately. Thanks in advance. Regards, (b)(6); (b)(7)(C); (b)(7)(F) **Domestic Investigations Branch** United States Marshals Service Mobile (b)(6); (b)(7)(C) (b)(6); (b)(7)(C); (USMS) From: Sent: Wednesday, March 25, 2020 3:02 PM (b)(6); (b)(7)(C); (b)(7)(F) To: (b)(6); (b)(7)(C); USMS) (b)(6); pusms.doj.gov>; (USMS) usms.doj.gov>; @usms.doj.gov>; (b)(6); (b)(7)(C); (b)(7)(F) (USMS (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); @usms.doj.gov> USMS) Subject: BWC Documents Hello everyone, Attached is the updated version of the documents as of today. Please let me know of any changes you would like made. Best, (b)(6); (b)(7)(C); (b)(7)(F) **Investigative Operations Division** United States Marshals Service (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)





VIDEO RETENTION SYSTEM (VRS) GOVERNANCE DOCUMENT



Version 1.2

02/24/2020

Prepared by:

Information Technology Division (ITD)

Release Notes

Version	Date	Description	Author
1.0	02/14/2020	Initial Draft	
1.1	03/10/2020	Update to roles and tags	(b)(6); (b)(7)(C); (b)(7)(F)
1.2	04/01/2020	Final updates to tags, tweak verbiage	CAN /V

Table of Contents

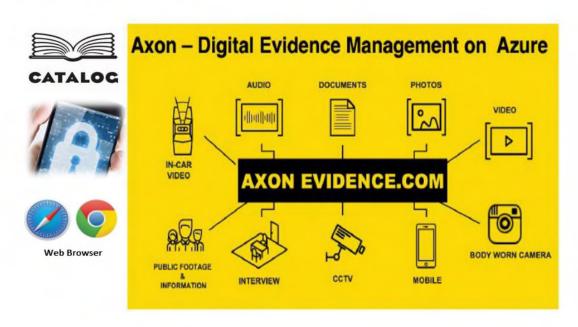
USMS VRS Overview	4
1.0 Governance Overview	5
2.0 Account Management Governance	5
2.1 Account Management Standards	5
2.1.1 Standard Account Provisioning, Modification and Deprovisioning	5
2.1.2 Privileged Account Provisioning, Modification and Deprovisioning	5
2.2 Account Management Changes	6
3.0 System Architecture Governance	7
3.1 System Architecture Standards	7
3.1.1 System Description	7
3.1.2 System Diagram	7
3.2 System Architecture Changes	8
4.0 Data Standards Governance	8
4.1 Data Standards	8
4.2 Data Standards Changes	9
Appendix 1 – USMS VRS Roles & Executive Approvers	10
Appendix 2 – Categories & Tags	11
Categories	11
Tags	11
Appendix 3 – USMS VRS Roles & Permissions	12

USMS VRS Overview

The United States Marshals Service (USMS), in conjunction with the recently announced Department of Justice (DOJ) Body Worn Camera (BWC) Pilot program, the Investigative Operations Division (IOD), Information Technology Division (ITD), Office of General Counsel (OGC) and other USMS Task Force Officer (TFO) partners have created a multiple workload initiative to support the DOJ mandate by implementing a solution to support the DOJ BWC Pilot Program that will allow federally deputized TFOs from state and local agencies to use BWCs while serving arrest warrants, other planned arrest operations, and during the execution of search warrants. For Workload 1, the USMS will be standing up the USMS Video Retention System (VRS) hosted on the Axon Evidence.com platform.

Advantages of USMS-VRS on Axon's Evidence.com

- ✓ Axon BWC used by 100K LEO at 6K agencies = 53 Petabytes of data
- √ 85% major cities and 40 major prosecutor offices including 12K US Attorneys
- Multiple jurisdictions in pilot site cities.
- ✓ SaaS Service built on Azure Gov Cloud with CJIS Compliance and encryption transit/rest
- ✓ Primarily stores evidence (we use for Taser events today)
- ✓ Mobile application primary interface but option for desktop with separate client option available (used for Pro users)
- ✓ Secure Portal upload (FBI/USAO uses in large public data requests video on public bombing etc. and for non-Axon LEO uploads
- ✓ Built in analytics and data management options move data less, audit, track, catalog
- ✓ Wide data/file type support also may include GPS/live stream data with auto activation and evidentiary time stamps



1.0 Governance Overview

The purpose of this document is to outline the system governance standards for the USMS Video Retention System (VRS).

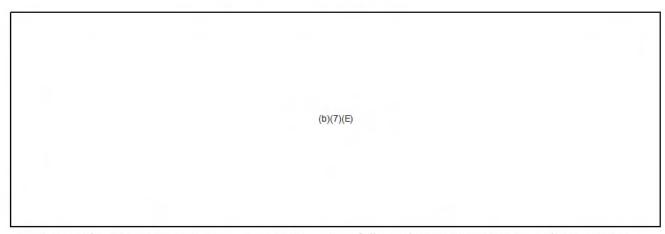
2.0 Account Management Governance

2.1 Account Management Standards

In accordance with USMS Policy Directive 12.3, Information Technology Account Management, access to all USMS systems must be granted via a defined process that documents the request. This section of the

USMS VRS Governance document outlines the account management standards that govern how accounts are provisioned, managed and deprovisioned.
2.1.1 Standard Account Provisioning, Modification and Deprovisioning Access, modification and deletion of access to the USMS VRS will be facilitated using the standard ITD USM-169, <u>User Access Request</u> process.
(b)(7)(E)
Service Levels: USMS VRS account management process follows the USMS ITD Service Delivery service levels for account requests.
Steps for the granting, modifying and deleting of account access to the USMS VRS can be found as an appendix to the <u>USMS Account Management Standard Operating Procedures</u> .
2.1.2 Privileged Account Provisioning, Modification and Deprovisioning Access, modification and deletion of access to the USMS VRS will be facilitated using the standard ITD USM-169P, <u>Privileged Access Request and Certification Form</u> process.

(b)(7)(E)



Service Levels: USMS VRS account management process follows the USMS ITD Service Delivery service levels for account requests.

Steps for the granting, modifying and deleting of privileged account access to the USMS VRS can be found as an appendix to the <u>USMS Account Management Standard Operating Procedures</u>.

2.2 Account Management Changes

Changes to the management of VRS account provisioning, deprovisioning and modification may occur from time to time. These changes may occur due to changes in Service Desk or System Administrator responsibilities, addition or deletion of roles that require approval or established service levels, *etc*.

Changes to the account management process will be facilitated by request to the ITD Information System Owner and the USMS VRS Operational and Administrative Business Owners. Changes will be evaluated and one of the following courses of action will be taken:

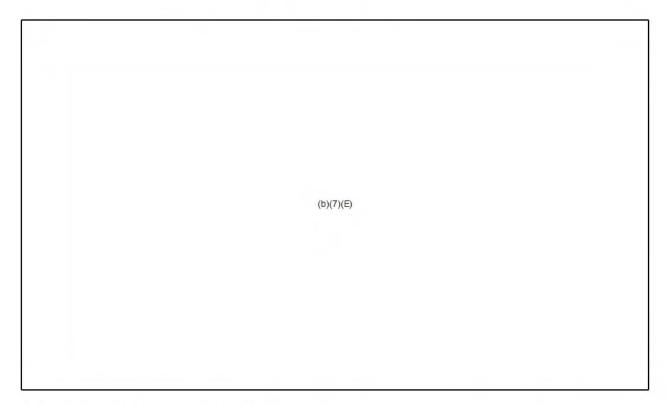
- 1. <u>Action as soon as practicable</u>: Small account management changes such as changes to verbiage in an SOP.
 - a. <u>Example Criteria</u>: Low to no coordination needed and no impact to security posture/accreditation.
- Action through an ITD Change Management request: Medium account management changes such
 as change to executive approvers, adding roles or groups with similar permissions, small changes to
 account request systems, etc.
 - a. <u>Example Criteria:</u> Low to medium coordination needed, small code changes. Less than 160 hours to resolve, minor impact to security posture/accreditation.
- Action through an ITIM/SDLC action: Large account management changes such as any extensive coding changes to the account request systems, changes to the account management process, requests for change to service levels
 - a. <u>Example Criteria:</u> Medium to high coordination needed, large code changes to account request systems, medium to high impact to security posture/accreditation. Over 160 hours of effort to resolve.

3.0 System Architecture Governance

3.1 System Architecture Standards

-	1 1	-	The second second	D		
4		1	/STAM	Descr	Int	ınn
J.		-	y J L C I I I	DCJCI	DL	1011

The USMS VRS platform is hosted on the Axon Inc.'s Digital Ev formerly Evidence.com. The platform is hosted in the	(b)(7)(E)	in an
nstance of Azure that is provisionally accredited by 3PAO to F		
	_	
Authentication:		
(b)(7)(E)		
End User Connection:		
(b)(7)(E)		1 73
A more thorough system description can be found in the Tech	nical Design Docume	ent located here.
3.1.2 System Diagram		
(b)(7)(E)		



3.2 System Architecture Changes

Changes to the VRS architecture may become necessary. These changes may occur due to addition of capability or tools, changing of base infrastructure aspects like ports, protocols or connections, or changes due to requirements by higher level

Changes to the system architecture will be facilitated by request to the ITD Information System Owner and the USMS VRS Operational and Administrative Business Owners. Changes will be evaluated and one of the following courses of action will be taken:

- 1. <u>Action through an ITD Change Management request</u>: Medium architecture changes such as firewall requests, *etc*.
 - a. <u>Example Criteria:</u> Low to medium coordination needed. Less than 160 hours, minor impact to security posture/accreditation.
- 2. Action through an ITIM/SDLC action: Large system architecture changes such as
 - a. <u>Example Criteria:</u> Medium to high coordination needed, medium to high impact to security posture/accreditation. Over 160 hours of effort to resolve.

4.0 Data Standards Governance

4.1 Data Standards

In order to ensure consistent system behaviors and accurate reporting, data standards have been developed for the data entry fields in the USMS VRS.

The table below represents the fields that are available in the USMS VRS and the standard data that will be input in the system.

Evidence				
Field	Description	Data Standard	Required?	
	(b)	(7)(E)		

Cases			
Field	Description	Data Standard	Required?
	(b)(7)(E)	

4.2 Data Standards Changes

Changes to VRS data entry standards may occur from time to time. These changes may occur due to additional necessary tags, changes to group names, etc.

Changes to data entry standards will be facilitated by request to the ITD Information System Owner and the USMS VRS Operational and Administrative Business Owners. Changes will be evaluated and one of the following courses of action will be taken:

- 1. <u>Action as soon as practicable</u>: Small data standards changes such as new tags being required to be entered, for reporting, *etc*.
 - a. <u>Example Criteria</u>: Low to no coordination needed and no impact to security posture/accreditation.
- Action through an ITD Change Management request: Medium account management changes such
 as change to executive approvers, adding roles or groups with similar permissions, small changes to
 account request systems, etc.
 - a. <u>Example Criteria</u>: Low to medium coordination needed, small code changes. Less than 160 hours to resolve, minor impact to security posture/accreditation.

Appendix 1 – USMS VRS Roles & Executive Approvers

The following table outlines the user roles available in the USMS VRS system, a description of that role and, whether an executive approval is needed and who the Executive approver is.

General - Non Admin Roles

Role	Description	E	Executive Approver
	(b)(7)(E)		

Privileged - Admin Role

Role	Description	E	Executive Approver
Admin	Administrative access to the VRS	(b)(7)(E)	

Appendix 2 – Categories & Tags

The following two tables outline the Categories that have been set up in the USMS VRS

Categories

Category	Description	Retention
	(b)(7)(E)	
1,		
Α -		

Tags

Tag	Description	
	(b)(7)(E)	

Appendix 3 – USMS VRS Roles & Permissions

		Pro	Pro	Pro	Pro	Basic	Pro	Basic	
Role Area	Role Setting	Admin	HQ Oversight	IOD Operations	Operational Command	Mission	TF Commander	User	Description
Login Access									
Login Access									
Login Access									
Login Access									
User Access									
User Access									
User Access									
User Access									
User Access									
Admin Access							(b)(7)(E)		
Admin Access									
Admin Access									
Admin Access									
Admin Access									

Admin Access	
Aumin Access	
Admin Access	
Admin Access	
Admin Access	
Aumin Access	
Search Access	
Search Access	
Search Access	
	(b)(7)(E)
Search Access	
Search Access	
Search Access	
Evidence Creation	1
Evidence dicution	
Friday Constinu	
Evidence Creation	
Evidence	
Evidence Management	
Evidence Management	
Evidence Management	
Management	
Management Evidence	
Management Evidence	
Management	

Management Evidence Management		
Evidence Management	Evidence	
Evidence Management Evidence Management	Management	
Evidence Management Evidence Management	Fyidence	
Evidence Management	Management	
Management Evidence Evidence Management Evidence Management Evidence Management Evidence Management		
Evidence Management	Evidence	
Management Evidence Management	Management	
Management Evidence Management	Evidence	
Management Evidence Management	Management	
Evidence Management		
Evidence Management	Management	
Evidence Management	Evidence	
Management Evidence Management	Management	
Management Evidence Management	5.11	
Evidence Management		
Management	ivianagement	
Evidence Management		
Evidence Management	Management	
Evidence Management Evidence Management Evidence Management Evidence Management Evidence Management Evidence Management	Evidence	(b)(7)(E)
Evidence Management Evidence Management Evidence Management Evidence Management Evidence Management	Management	
Evidence Management Evidence Management Evidence Management Evidence Management Evidence	Evidence	
Evidence Management Evidence Management Evidence Management Evidence Management	Management	
Evidence Management Evidence Management Evidence Management Evidence Management	Evidones	
Evidence Management Evidence Management Evidence Evidence	Management	
Evidence Management Evidence Sevidence	3	
Evidence Management Evidence Sevidence		
Evidence Management Evidence Sevidence		
Evidence Management Evidence Sevidence	Evidence	
Evidence Management Evidence	Management	
Management Evidence		
Management Evidence		
Management Evidence	Evidence	
Evidence	Management	
Evidence Management		
ivianagement	Evidence	
	ivianagement	

Evidence
Management
Case
Management
Case
Management
Case
Management
Case
Management
Case
Management
Case
Management
Casa
Case
Management
Case
Management
Case
Management
Case
Management
Case
Management
Citizen Management
ivianagement
Citizen
Management
Citizen
Management
The second second

Citizen Management	
Email Notification	
Preferences	
Email Notification Preferences	(b)(7)(E)
Email Notification Preferences	
riciciences	

UNCLASSIFIED // FOR OFFICIAL USE ONLY

VIDEO RETENTION SYSTEM (VRS) ORIENTATION GUIDE



Version 1.3

04/01/2020

Prepared by:

Information Technology Division (ITD)

Release Notes

Version	Date	Description	Author
1.0	02/13/2020	Initial Draft	
1.1	02/27/2020	Updates to sections on cases and evidence definition	(b)(6); (b)(7)(C); (b)(7)(F)
1.2	03/23/2020	Updates based on experiences from pilot site training	
1.3	04/01/2020	Final tweaks	

Table of Contents

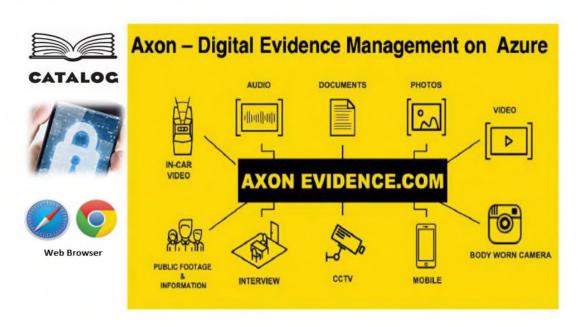
USMS VRS Overview	4
1.0 General Usage	5
1.1 System Access & Logon	5
1.1.1 Access the USMS VRS	5
1.2 General Navigation	7
1.2.1 Dashboard	7
1.2.2 Navigation Bar	8
2.0 Body Worn Camera Data Request	10
2.1 Axon Partner Data Request	10
2.1.1 Partner Agency Sharing Setup	10
2.1.2 Axon Partner Data Sharing to the USMS	13
2.2 Non-Axon Partner Data Request	13
2.2.1 Non-Axon State & Local Data Invitation (USMS Action)	13
2.2.2 Non-Axon State and Local Data Upload (Task Force Action)	15
2.2.3 Non-Axon State & Local Data Acceptance (USMS Action)	17
2.2.4 Non-Axon Data Requests Management	19
3.0 Body Worn Camera Data Management	21
3.1 Case Creation	21
3.2Case Data Management	23
4.0 Body Worn Camera Image Processing	27
4.1 VRS Markers and Clips	27
4.1.1 Reviewing Video	27
4.1.2 Create Markers and Clips	28
4.2 Video Redaction	30
Appendix 1 – USMS VRS Roles	31
Annondix 2 - VPS Data Standards	22

USMS VRS Overview

The United States Marshals Service (USMS), in conjunction with the recently announced Department of Justice (DOJ) Body Worn Camera (BWC) Pilot program, the Investigative Operations Division (IOD), Information Technology Division (ITD), Office of General Counsel (OGC) and other USMS Task Force Officer (TFO) partners have created a multiple workload initiative to support the DOJ mandate by implementing a solution to support the DOJ BWC Pilot Program that will allow federally deputized TFOs from state and local agencies to use BWCs while serving arrest warrants, other planned arrest operations, and during the execution of search warrants. For Workload 1, the USMS will be standing up the USMS Video Retention System (VRS) hosted on the Axon Evidence.com platform.

Advantages of USMS-VRS on Axon's Evidence.com

- ✓ Axon BWC used by 100K LEO at 6K agencies = 53 Petabytes of data
- √ 85% major cities and 40 major prosecutor offices including 12K US Attorneys
- ✓ Multiple jurisdictions in pilot site cities.
- ✓ SaaS Service built on Azure Gov Cloud with CJIS Compliance and encryption transit/rest
- ✓ Primarily stores evidence (we use for Taser events today)
- ✓ Mobile application primary interface but option for desktop with separate client option available (used for Pro users)
- ✓ Secure Portal upload (FBI/USAO uses in large public data requests video on public bombing etc. and for non-Axon LEO uploads
- ✓ Built in analytics and data management options move data less, audit, track, catalog
- ✓ Wide data/file type support also may include GPS/live stream data with auto activation and evidentiary time stamps



1.0 General Usage

1.1 System Access & Logon

To access to the USMS Video Retention System (VRS), USMS employees must access the system utilizing the following:

- USMS laptop or desktop
- Connected to the USMS network either in the office or remotely via VPN

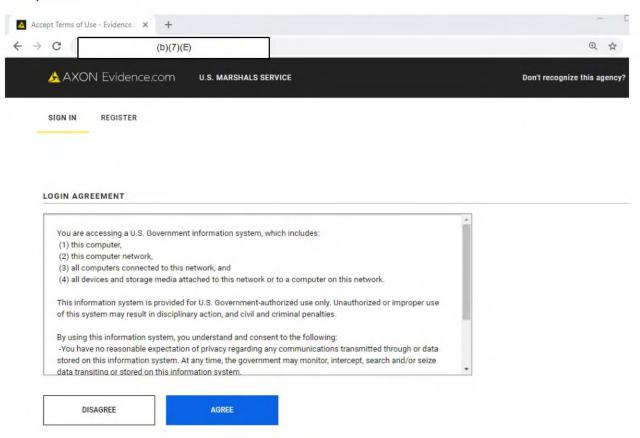
Additionally, while the Internet Explorer browser will work with the USMS-VRS, the Chrome Internet browser will work more reliably.



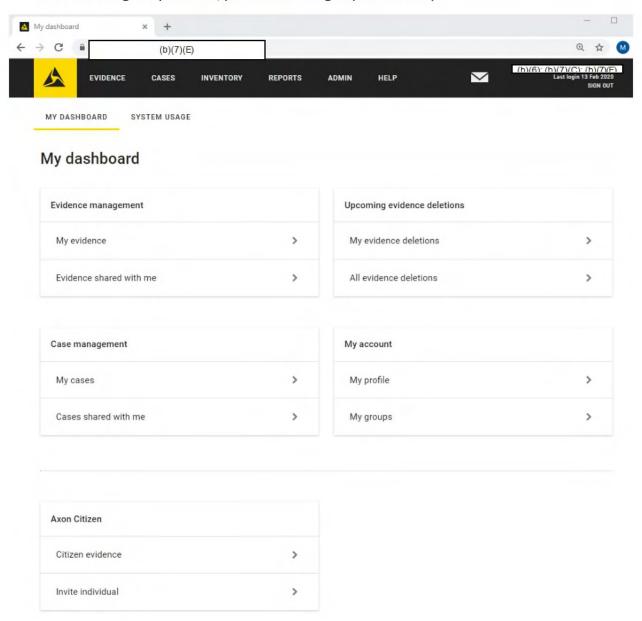
The system uses your HSPD-12 PIV card to access the VRS.

1.1.1 Access the USMS VRS

- 1. Open your Chrome browser. In the web address window type in (b)(7)(E) and press enter
- 2. You will get a screen indicating you will be redirected, no action is necessary
- 3. At the US Government Login Agreement Screen, read the agreement and select Agree to enter the system.



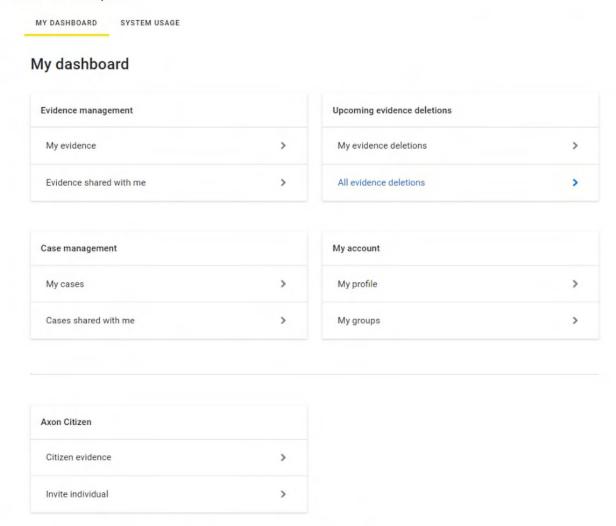
4. The system will take you to your personalized dashboard, displaying functions and features that you have access to given your roles, permissions and group memberships



1.2 General Navigation

1.2.1 Dashboard

The dashboard home screen of the USMS VRS provides shortcuts to the most used portions of the USMS VRS system. What you may see will depend on the role that you were set up with via the USM-169, User Access Request.



The below table lists the dashboard options and their functions

Evidence Management				
My Evidence	View of all pieces of information where the currently logged in user is the Owner			
Evidence Shared With Me	View of all pieces of information that were shared to the currently logged in user, either from an internal user (USMS) or another partner agency that uses Axon's Evidence.com (e.g. Wichita Police Department)			
	Upcoming Evidence Deletion			
My Evidence Deletions	View of all pieces of information scheduled for deletion where the currently logged in user is the Owner			
All Evidence Deletions	View of all pieces of information scheduled for deletion where the currently logged in user has permission to see the data			
	Case1 ¹ Management			
My Cases	View of all VRS Cases where the currently logged in user is the Owner			
Cases Shared with Me	View of all VRS Cases that were shared to the currently logged in user, either from an internal user (USMS) or another partner agency that uses Axon's Evidence.com			
	My Account			
My Profile	View of currently logged in user's profile data			
My Groups	View of currently logged in user's groups that are monitored or a member of			
	Axon Citizen (Restricted)			
Citizen Evidence (Restricted) View of all data that has been submitted by State and Local Task Force partners not on the Axon platform (Restricted to specific roles/users)				
Invite Individual (Restricted)	Capability to solicit data from State and Local Task Force partners not on the Axon Platform (Restricted to specific roles/users)			

Table 1 Dashboard Options Description

1.2.2 Navigation Bar

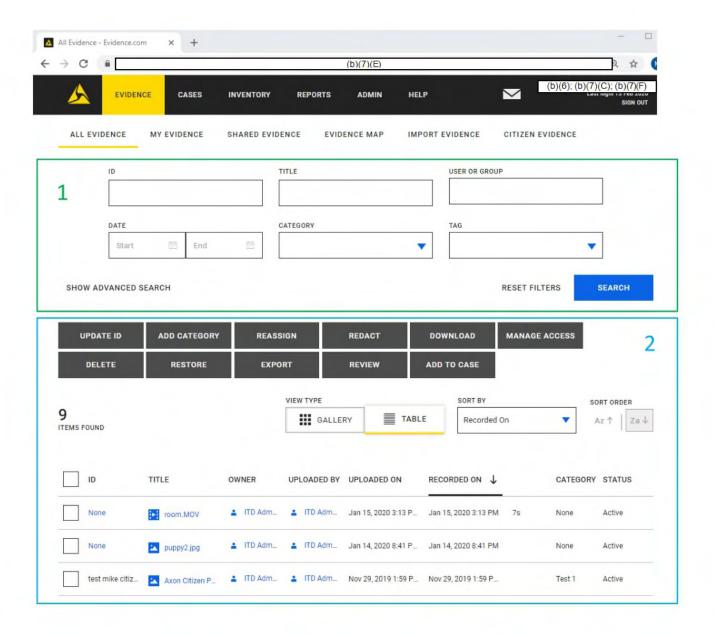
The navigation bar at the top of the website is another way to access data stored on the USMS VRS. Selecting the different options on the navigation bar will get you to views of all the data that you have access to, security trimmed to what you have permission to see via your role or permissions. **Note**: Some of these options may not appear on your personal navigation bar depending on your role!

The following is the navigation bar along with descriptions of the functions



Evidence: Clicking the evidence option in the tool bar will bring you to the All Evidence screen as shown below

¹ A VRS "Case" is simply a logical grouping of pieces of evidence. The VRS is not intended to be a case management system.



- 1. Section 1 in green above highlights the search area where you can filter the results of data that you have access to
- 2. Section 2 in blue above highlights the actions that can be taken on the and the selectable data itself

2.0 Body Worn Camera Data Request

The following section outlines the process to make requests for data from both Axon and Non-Axon State and Local Task Force partner agencies

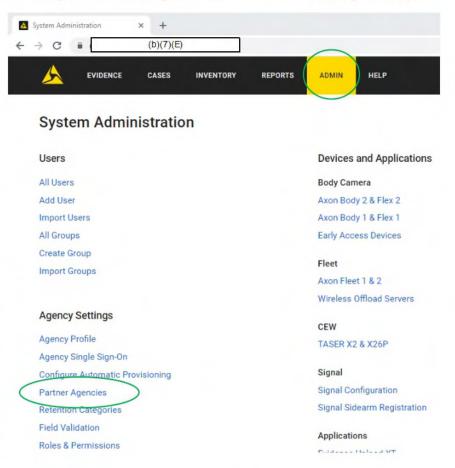
2.1 Axon Partner Data Request

This section outlines how to create a sharing connection to a State or Local agency that uses Axon, Inc.'s Body Worn Cameras and Evidence.com.

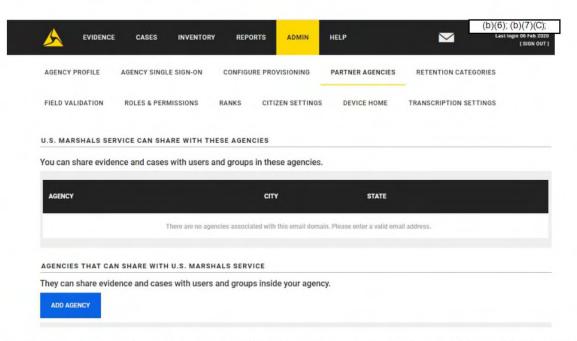
2.1.1 Partner Agency Sharing Setup

Prior to any data sharing, a one-time partner agency sharing setup must be initiated. **Note**: Creating a partner agency request requires special privileges.

- 1. Log on to the USMS-VRS at (b)(7)(E)
- 2. Click on the Admin option on the navigation bar; Select the Partner Agencies option

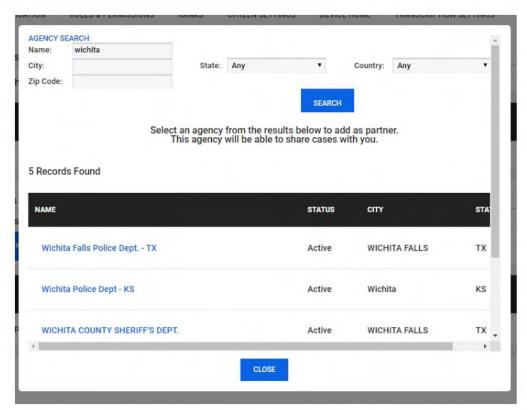


3. On the Partner Agencies screen, click the Add Agency button

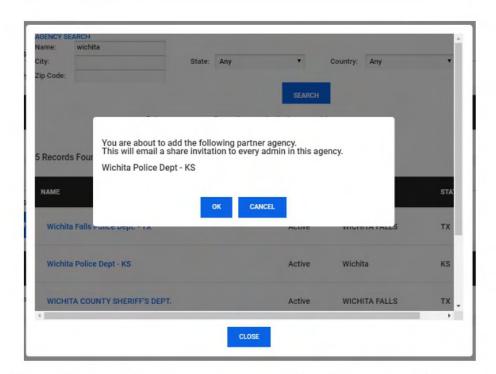


4. On the search screen type in the name of the partner agency and select the blue Search button.

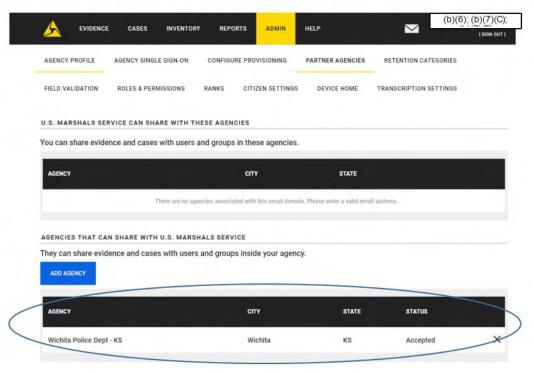
Note: Partial names can be used to search across states



5. Find your appropriate State or Local Task force police department and click the entry. Select the OK button to make the sharing request.



6. Once the participating Task Force agency has accepted the sharing request, the partner will now show in the "Agencies that can share with the U.S. Marshals Service" area of the Partner Agencies screen. Note: This means that this partner agency only has access to see USMS's list of users and groups in the Axon Evidence.com system, they have NO access to see our data.



2.1.2 Axon Partner Data Sharing to the USMS

The partner agency will follow their internal procedures for sharing data, selecting a USMS user or Group to share to. More detail on how to do this is in the Axon Evidence Handbook.

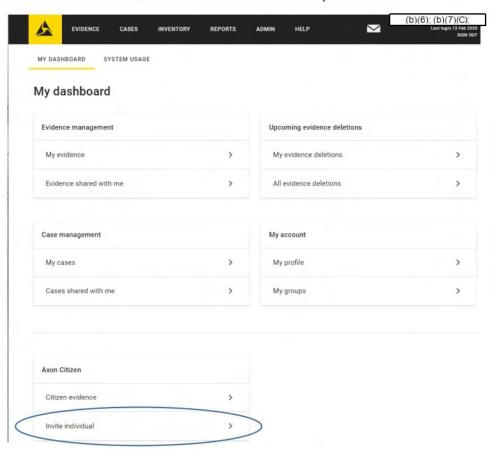
2.2 Non-Axon Partner Data Request

This section covers how to make a data request to USMS State and Local partners that do not use Axon's Evidence.com platform to manage their Body Worn Camera data.

2.2.1 Non-Axon State & Local Data Invitation (USMS Action)

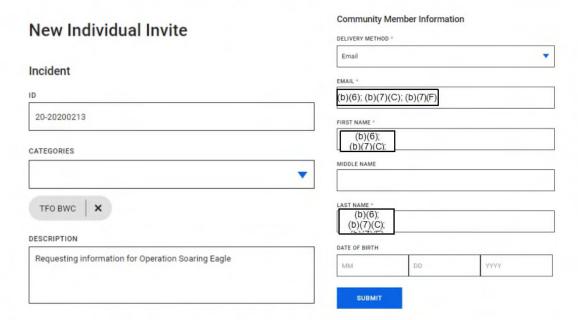
To solicit data from the non-axon State or Local partner, perform the following steps:

- 1. Log on to the USMS-VRS at (b)(7)(E)
- 2. Click "Invite Individual" under the Axon Citizen area on the My Dashboard

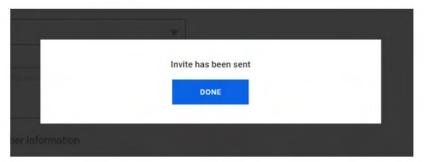


- 3. On the "New Individual Invite" screen, input the following information:
 - a. ID: Enter the "USMS-" plus the FID
 - b. Category: Select "TFO BWC"
 - c. Description: Enter a description you'd like to include in the request. **Note**: All data gets added to the audit log so ensure text is appropriate
 - d. Delivery Method: Select "Email"
 - e. Email: Enter the email address of the recipient
 - f. First Name: Enter the First Name of the Recipient
 - g. Last Name: Enter the Last Name of the Recipient

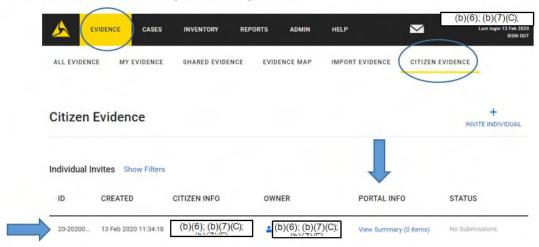
h. Note: Middle name and DOB are not required fields



- 4. Click the Submit button to initiate a sharing request
- 5. Click Done to complete the action



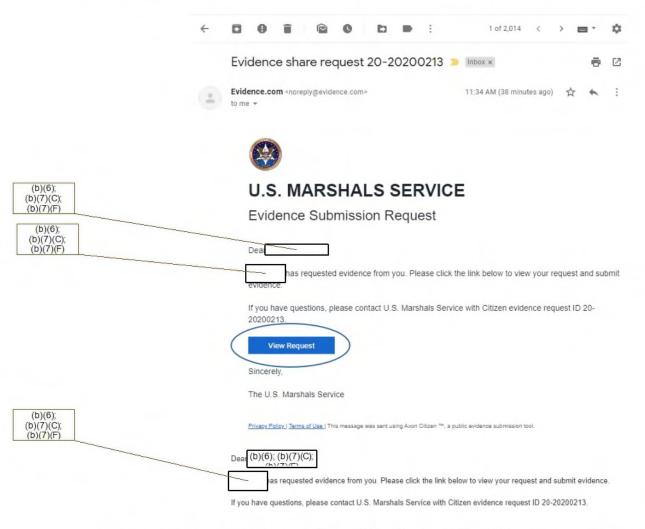
6. The data sharing request now shows in the VRS Evidence > Citizen Evidence portal along with information on whether any data was uploaded



2.2.2 Non-Axon State and Local Data Upload (Task Force Action)

The following are the procedures for the State and Local Task Force (non-USMS, non-Axon) officers to upload their data. This section assumes the above USMS action of initiating the Axon Citizen request has been initiated and also assumes that the TFO, or TFO state/local supervisor has gathered all relevant BWC footage and saved it to a folder.

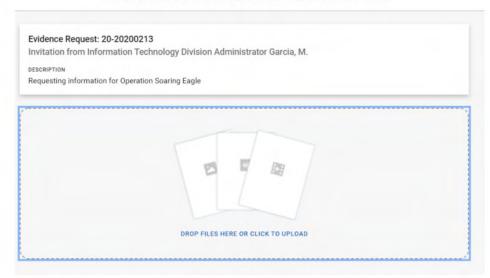
- 1. Individual that was sent the data request will have gotten an e-mail titled "Evidence share request USMS-FID"
- 2. In the middle of the e-mail there should be a blue button that says View Request, they will click that button



- 3. A new internet web browser window or tab will open on the TFO's computer, directing them to the Evidence submission portal for that particular request
- In the middle of the window is an area to either drop files on to or click to select them from a File Manager window. Multiple files can be selected using either method



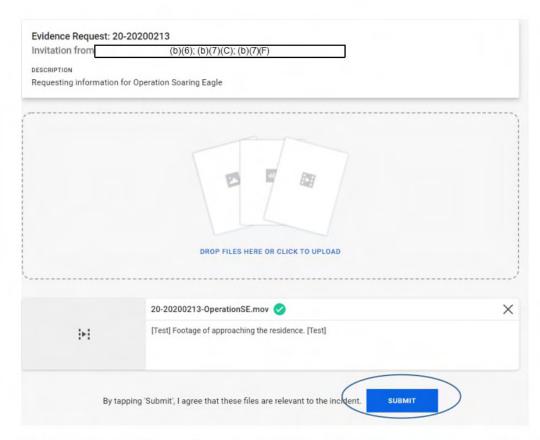
U.S. Marshals Service Evidence Submission Portal



5. If clicking to upload, browse to the file folder, highlight the files and click the Open button



6. If the TFO needs to add more files they may do so by repeating the previous steps. They may add a caption to the data (like local case numbers or other relevant data) and select the Submit button



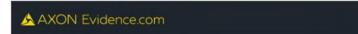
7. The TFO will receive a thank you message indicating the files have been submitted. They can close the window.

<u>Important Note</u>: The portal submission page is a one-time only link. Once data has been submitted for that link, if more relevant data is needing to be uploaded, a new data request from the USMS will need to be initiated.

2.2.3 Non-Axon State & Local Data Acceptance (USMS Action)

Before the USMS fully ingests the data that a non-Axon State and Local agency has uploaded, it must be reviewed and accepted or rejected. Below are the steps to triage the requested data:

- 1. When the partner completes their upload of the data to the Citizen portal, the initiator will receive an e-mail that there was a new submission requiring triage.
- 2. Click the "View Submission" link contained within the e-mail to sign in to the USMS VRS system to triage the data.

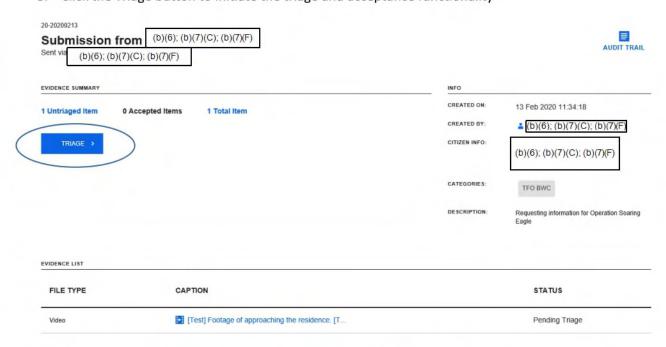




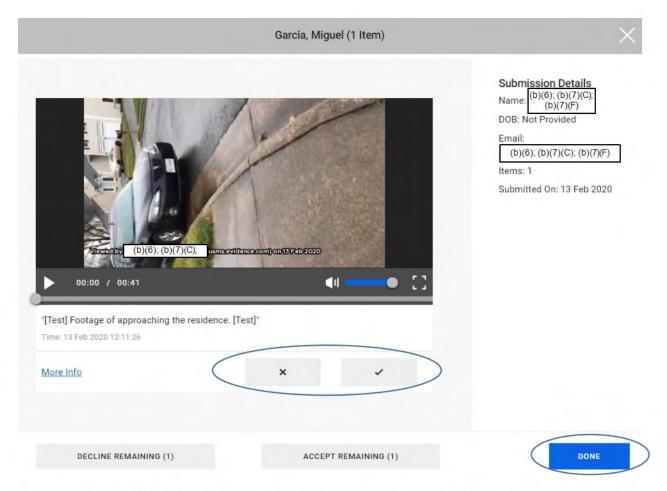
3. Click the Triage button to initiate the triage and acceptance functionality

VIEW SUBMISSION

Sincerely, The Axon Team



4. The next screen allows you to review the data and determine if it is relevant and/or usable.

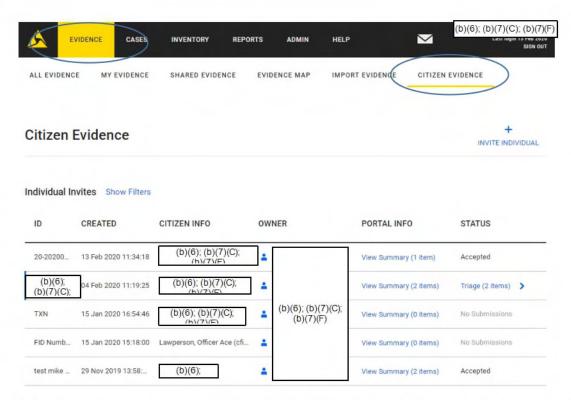


- 5. Select the Check Mark for all pieces of data that you wish to accept and ingest into the system or select the X to decline that piece of data.
- 6. **Note**: The Decline Remaining and the Accept Remaining buttons indicate how many pieces of data have not had a selection made.
- 7. When complete, click Done to complete the triage and acceptance process.

2.2.4 Non-Axon Data Requests Management

If you are unsure if a data request has been acted on you can use the Citizen Evidence portal in the VRS to see the status of the requests. Below are the steps to get to the portal:

- 1. Click the Evidence option at the top menu bar and select Citizen Evidence
- 2. You will see all non-Axon data requests that have been initiated and their statuses



3. Click the Show Filters and move the radio button to "Only My Portals" to show only data requests that you have initiated.

Under the status column if there is a status of "Triage (x items)" then there has been a submission that needs to be reviewed and accepted or rejected. A status of "No Submissions" means nothing has been uploaded yet.

3.0 Body Worn Camera Data Management

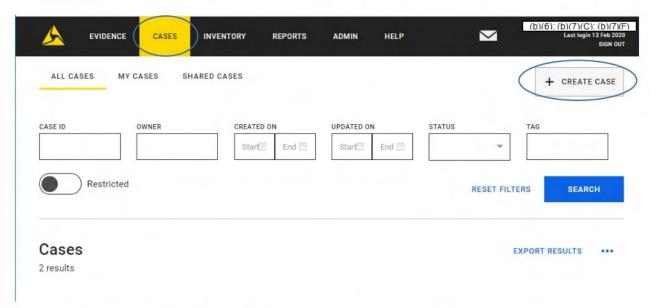
This section deals with the management of the data that we have received from the State and Local agencies, regardless of whether it came in from Axon or Non-Axon partners. The sections below outline Case creation, Evidence and Metadata updates.

3.1 Case Creation

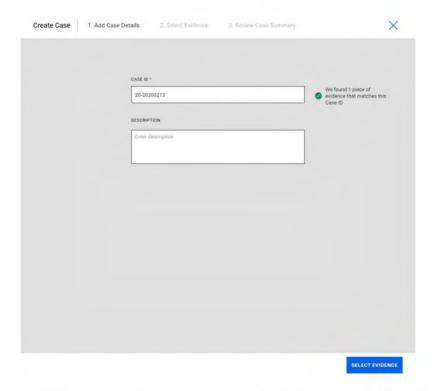
Case creation in the USMS VRS is geared toward logically grouping sets of data together to ease in searching and management. The Case functionality of VRS and Evidence.com are not intended to supersede or take the place of a USMS case management system, merely house the transient Federal records of the BWC footage captured by our Task Force partners.

To create a VRS case, perform the following steps:

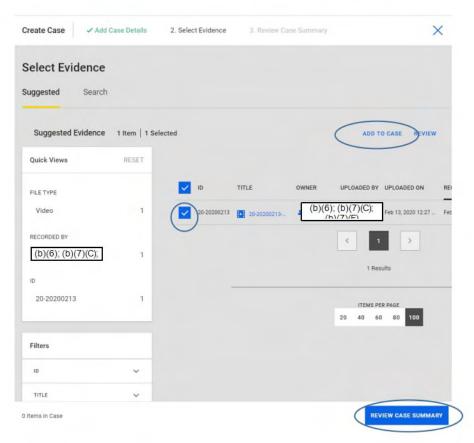
 Click the Cases option on the menu bar and click the Create Case button on the right hand side of the screen



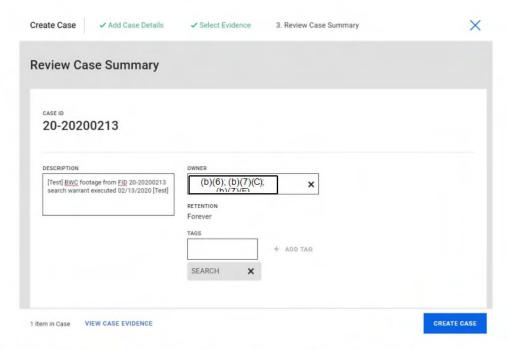
- 2. In the Case ID field, type in "USMS-" plus the FID, EG: USMS-12345678
- 3. The system will automatically start searching for data that has the same FID and will display any matches. Select the Select Evidence button



- 4. On the Select Evidence screen if there was a match it will be automatically displayed
- 5. Click the check box next to the data and select the "Add to Case" option to add the data to the Case



- 6. Select the Review Case Summary button to review final information and add description text, and any appropriate tags as outlined in Appendix 2.
- 7. Select Create Case.

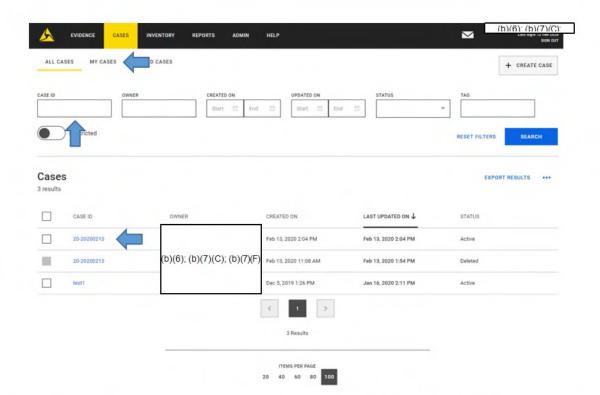


8. The VRS will take you to the Case Summary page for the newly created case.

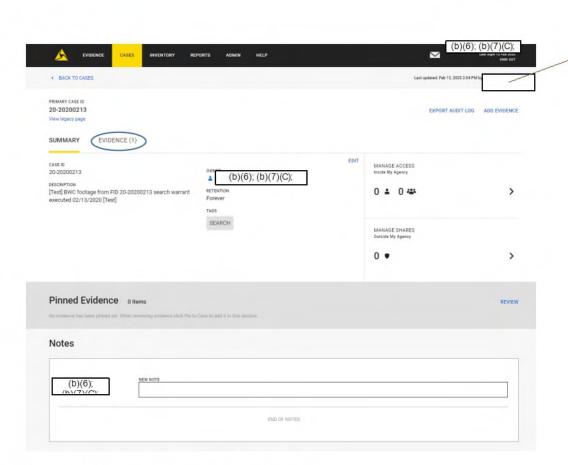
3.2Case Data Management

To ensure accurate reporting and system behavior the information about the data, i.e. the metadata, must be accurate. This section will outline how to enter, or update, the metadata used by the VRS.

- 1. First access the Cases capability by clicking the Cases option on the menu bar
- 2. You will be at the All Cases view where you can see all cases that you have permissions to.



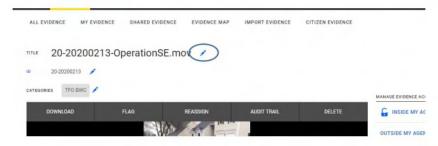
- 3. If you are the owner (creator) or assignee of a case you can click the My Cases option to see your cases, otherwise type the FID in to the Case ID search area to search for a case
- 4. Click the Case ID to enter the Case Summary screen
- 5. On the Case Summary screen you can see the Summary information as well as how many pieces of evidence are associated with this case.



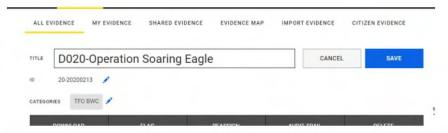
6. Click the Evidence link to see the associated evidence



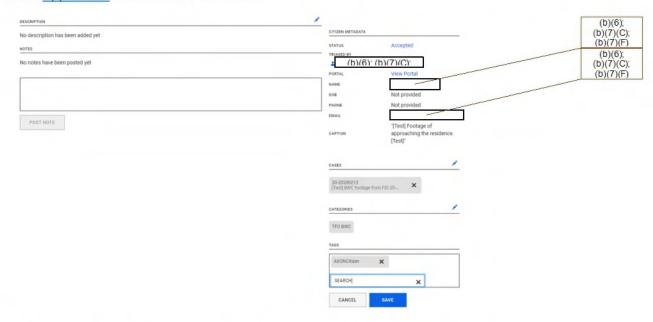
- 7. Click the Title of a piece of data to enter the Evidence Review screen.
- 8. On the Evidence Review Screen, ensure the Title of the piece of data conforms to the USMS required format as outlined in Appendix 2.



(b)(6); (b)(7)(C); (b)(7)(F) 9. Change the title by selecting the Pencil icon next to the title and inputting the correct information and clicking Save



10. Scroll to the bottom of the Evidence Review Screen. Ensure the required Tags are present and the appropriate Category is selected. If not, select the pencil icon next to each item and input the data as outlined in Appendix 2 and click Save when done.



- 11. An additional Description or Notes can be added by clicking the pencil icon and clicking save, or in the case of Notes, click the Post Note button.
- 12. Repeat steps 6 through 11 for each piece of data associated with the case

4.0 Body Worn Camera Image Processing

This section of the USMS VRS guide deals with the processing of the video files that will be ingested. This guide covers two aspects of video processing.

- Creation of Markers and Clips
- Redacting Video

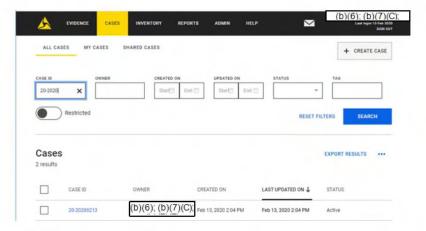
This guide covers the tools inherent in the VRS / Evidence.com toolset. If other capabilities or features are needed, the video must be exported and another tool used.

4.1 VRS Markers and Clips

This section outlines the methods for creating position markers and clips for video content. This section assumes video has already been uploaded and the appropriate metadata applied.

4.1.1 Reviewing Video

- 1. In the VRS, click the Cases option on the menu.
- 2. Type in the FID in the Case ID portion of the search section and click the appropriate Case ID listing in the results



3. On the Case Summary Screen click the Evidence option and then click the Title of the item you wish to process



4. On the Evidence Summary screen, on the right you will have a window which you can review the video.



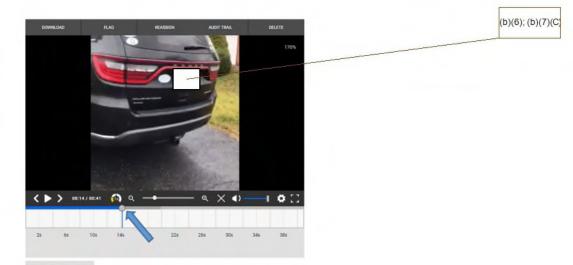
- 5. Use the Frame Back, Play and Frame forward buttons to play at normal speed or go frame by frame forward or backward.
- 6. Use the 1x, 2x, 4x options to increase or decrease the play speed.
- 7. Use the zoom and volume buttons to increase or decrease those options.
- 8. Use the gear button to increase or decrease the video resolution and the brackets button to enable or disable full screen mode.
- 9. Use the slider button to move the displayed video frame to the desired position.

4.1.2 Create Markers and Clips

This section covers how to create both position markers as well as clips from the video.

Markers

- 1. Access the desired video as outlined in the Video Review section above.
- 2. Use the right mouse button to select the slider button and scroll to the frame that you wish to place the marker at.
- 3. Click the Add Marker button to create a Marker as shown in the image below.



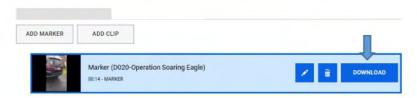
4. The Marker image will now appear under the video Add Marker and Add Clip buttons. Click the Pencil button to edit the Title of the Marker



5. Enter any desired descriptive text for the marker and click Save when done.



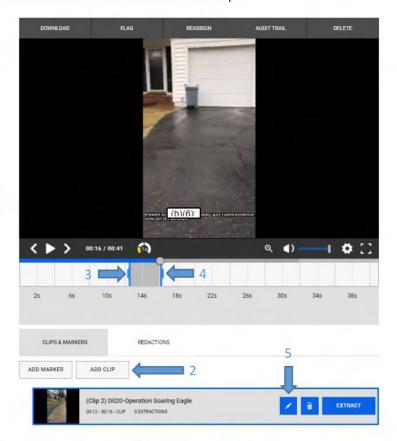
- 6. Now, when clicking the marker entry, no matter where the slider button is, it will go directly to the marked point.
- 7. Additionally, clicking the Download button on a marked point will download a still image from that marked point to your computer.



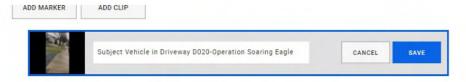
Clips

- 1. Access the desired video as outlined in the Video Review section above.
- 2. Click the Add Clip button.

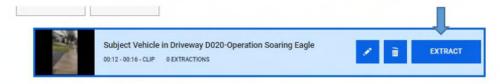
- 3. Slide the left blue slider to the desired start of the clip.
- 4. Slide the right blue slider to the desired end of the clip.



5. Click the Pencil icon to edit the title of the Clip and click Save



6. Click Extract to download a copy of the video Clip to your workstation



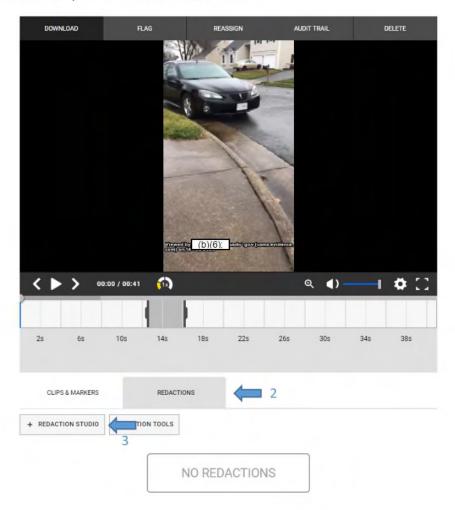
4.2 Video Redaction

This section outlines the methods and tools available for creating redacted video. This section assumes video has already been uploaded and the appropriate metadata applied as identified in the Case Management section.

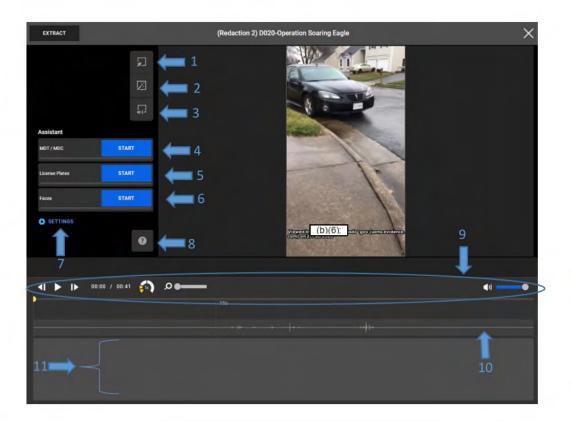
4.2.1 Redaction Studio Access

1. Access the desired video as outlined in the Video Review section above.

2. Click the Redactions option below the Video viewer.



3. Click the Redaction Studio button to launch a redaction session on the selected video.



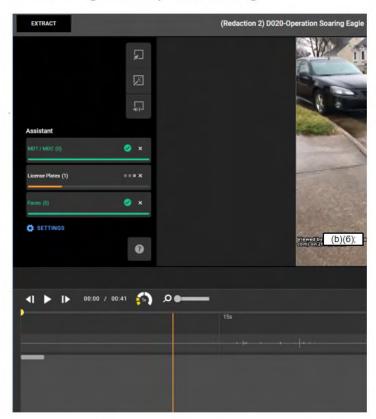
- 1. Manual Mask Function
- 2. Object Tracker Function
- 3. Audio Mask Function
- 4. Mobile Device Terminal / Mobile Digital Computer Tracker Automatic
- 5. License Plate Tracker Automatic
- 6. Faces Tracker Automatic
- 7. Settings button for Automatic/Artificial Intelligence options (4, 5, 6)
- 8. Help button, explaining screen options
- 9. Video play bar, speed, zoom, volume and cursor placement
- 10. Audio track
- 11. Object & Al indication bar (shows instances of objects and possible redactions)

4.2.2 Video Redaction Process

- 1. Click the Settings button under the AI Assistant options
- 2. Set the blur level for all 3 Al assisted areas as appropriate, select the Redact All check box(es) and click Save (note, this only selects what the Al finds, it does not redact those areas quite yet)

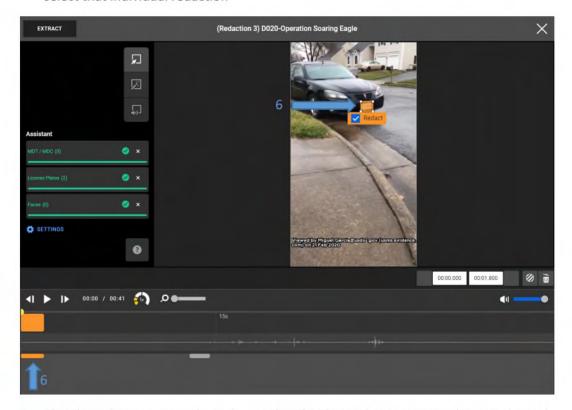


- 3. Click Start on all the appropriate AI assistant buttons to start the Artificial intelligence search for those areas.
- 4. You will see three dots indicating that the system is working



5. When your categories are done there will be a green check mark beside the category along with a number indicating the number of times that items in that category were discovered and where in the video they are

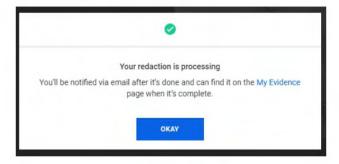
6. Clicking either the area on the screen that shows the redaction box or the item in the timeline will select that individual redaction



- 7. Play the video to ensure the redaction box for that redaction covers the area desired
- 8. Use the space bar or paus button to stop the play on a frame and use the redaction box anchor points to expand or move the redaction space for that frame.



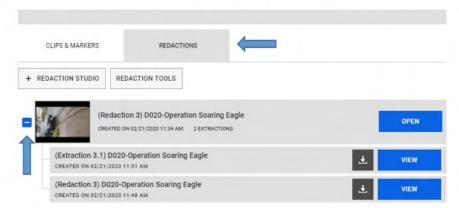
- 9. Move the video forward and backward to repeat steps 7 and 8 above.
- 10. When done click the Extract button at the top left of the screen to begin the redaction process.
- 11. Click Ok at the processing screen



- 12. Depending on the size of the video, the size of the redaction, the process could take a while.
- 13. The system will send an e-mail when complete



- 14. Either click the e-mail link or follow normal procedures for looking up pieces of video
- 15. Click the Redactions tab
- 16. You will now have an item under the redaction tab labeled with Redaction along with a check indicating the processed file associated with the redaction



- 17. Click View to watch the processed file
- 18. Click the down arrow to download a copy to your local machine

Appendix 1 – USMS VRS Roles

The following table outlines the user roles available in the USMS VRS system, a description of that role

Role	Description	
	(b)(7)(E)	

Appendix 2 – VRS Data Standards

This appendix deals with the data standards associated with the categories and tags associated with the system.

_						
1 -	+0	T	0	PI	0	-
Ca	16	- 2		11		
		$^{\circ}$	-		_	_

Category	Description	
	/b)/7//E)	
	(b)(7)(E)	
r As		
177		

Tags

Tag	Description
	(b)(7)(E)

(b)(7)(E)	

From: Young, Jakari

Sent: Tue, 12 Jan 2021 22:18:29 +0000

To: (USMS)

Cc:

Subject: RE: BWC follow up

(b)(6); (b)(7)(C); (b)(7)(F)

No worries! Thanks for the update.



Be Safe, Be Well, Be Blessed.. Jakari E. Young

Chief of Police

Daytona Beach Police Department | 129 Valor Blvd

Main: (386) 671-5100 Direct: (b)(6): (b)(7)(C)

(b)(6); (b)(7)(C) **Odbpd.us**



From: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7)(F) @usdoj.gov>

Sent: Tuesday, January 12, 2021 4:01 PM **To:** Young, Jakari (b)(6): (b)(7)(C) DBPD.US>

Subject: RE: BWC follow up

[EXTERNAL EMAIL. EXERCISE CAUTION.]

Hi Jakari,

I hope all is well over there. We all have our hands full right now it seems. I just wanted to give you a heads up on the BWC's that HQ is getting ready to roll our their plan to onboard agencies and I should know something sooner that later. I will be in our HQ next week and I am going to inquire to see what I can find out. I will keep you posted. Sorry this is taking so long to get going.

(b)(6); (b)(7)(C):

From: Young, Jakari (b)(6): (b)(7)(C) @DBPD.US> Sent: Friday, November 20, 2020 2:03 PM

To: (b)(6); (b)(7)(C); (b)(7)(F) USMS) (b)(6); (b)(7)(C); usms.doj.gov>

Subject: RE: BWC follow up

Afternoon (b)(6);

Sorry for the delay. Just a few questions for clarification in reference to this BWC policy.

II. USE OF BODY WORN CAMERAS DURING FEDERAL TASK FORCE OPERATIONS:

must deactivate their BWCs when the scene is secured as determined by the federal supervisor on the scene

For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.

The policy reads that a BWC will be off once the scene is secure, you will not allow a BWC on during a search for evidence?

Are you concerned at all about being accused of stealing or planting evidence?

TFOs are prohibited from activating their BWC if the TFO is using specialized or sensitive investigative techniques, operating in a sensitive area, or working in an undercover or covert status on behalf of the federal task force

TFOs generally shall not use their BWCs to record any activities related to investigations involving public corruption, medical facilities, national security, or other sensitive investigations

Does this mean when an arrest is about to be effected or just doing the investigation leading up to? And who determines or what determines sensitive investigations?

The Department's policy of permitting the limited use of BWCs on task forces does not apply to highly specialized or sensitive operations or groups as determined by the federal agency sponsoring the task force.

Are the US Marshals considered part of this group?

IV. FEDERAL RECORDS:

B. Expedited Public Release:

If TFO BWC recording(s) depict conduct committed solely by a TFO resulting in serious bodily injury or death of another

Does this apply only when he is acting as a TFO for the federal agency or anytime he is involved in something (like if he assists DBPD on something? Also it states solely, what occurs if more TFO's or agents themselves are involved?

Thanks,



Be Safe, Be Well, Be Blessed.. Jakari E. Young

Chief of Police







From: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7)(F) @usdoj.gov>

Sent: Thursday, November 12, 2020 2:15 PM

To: Young, Jakari (b)(6): (b)(7)(C) DBPD.US>

Subject: BWC follow up

[EXTERNAL EMAIL, EXERCISE CAUTION.]

Good afternoon,

I wanted to follow up to see if you have had a chance to review the DOJ BWC policy. As an agency, we are continuing to finalize our processes. I am waiting on further guidance from our headquarters and once I have the additional guidance and documents, I will be sure to pass them along. I do know that the first step will be to gain concurrence from your agency that you agree to what is in the policy before we can begin to talk about moving forward. Please take as much time as needed to review the policy and I will be sure to keep in touch as our internal program progresses. Please let me know if you should have any questions at all. Talk with you soon.

(b)(6); (b)(7)(C); (b)(7)(F)

United States Marshals Service Florida/Caribbean Regional Fugitive Task Force

(b)(6); (b)(7)(C); (b)(7)(F)

USDOJ.GOV

This information is for U.S. Marshals Service LIMITED OFFICIAL USE and is LAW ENFORCEMENT SENSITIVE. E-mails are protected under the Electronic Communications Privacy Act, 18 U.S.C. 119 Sections 2510, 2511, and 2521. Dissemination to non-law enforcement sources is strictly prohibited without prior approval. Any inquiries concerning this information should be directed to the sender of this email.

Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.

Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.

(b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS) To: Subject: RE: DOJ Interim BWC policy Attachments: BWC DOJ Interim Policy.pdf Good morning, Attached is the BWC DOJ Interim Policy. Please let me know if there are any other documents you would like me to provide. Best, (b)(6); (b)(7)(C); (b)(7)(F) **Investigative Operations Division** United States Marshals Service (b)(6); (b)(7)(C) C: (USMS) (b)(6); (b)(7)(C); (Dusms.doj.gov> From: (b)(6); (b)(7)(C); Sent: Friday, August 21, 2020 11:12 AM $(USMS)^{(b)(6); (b)(7)(C);}$ @usms.doj.gov> SMS) (b)(6); (b)(7)(C); usms.doj.gov> Subject: RE: DOJ Interim BWC policy (b)(6); (b)(7)(C); Can you provide the DOJ BWC policy to (b)(6): Thanks! (b)(6); (b)(7)(C); (b)(7)(F) From: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7 Sent: Friday, August 21, 2020 11:08 AM USMS) (b)(6); (b)(7)(C); (b)(7)(F) To: (b)(6); (b)(7)(C); usms.doj.gov> Subject: RE: DOJ Interim BWC policy That's the one I wanted to share the DOJ Interim policy, not ours. Do you have the most updated copy of that one that can be shared? Thanks man. (b)(6); (b)(7)(C); USMS) (b)(6); (b)(7)(C); (b)usms.doj.gov> Sent: Friday, August 21, 2020 11:06 AM To: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7)(C); (b)(7)(F) (D)(7)(F)

(b)(6); (b)(7)(C); (b)(7)(F)

USMS)

Fri, 21 Aug 2020 15:16:39 +0000

From:

Sent:

Subject: RE: DOJ Interim BWC policy

I have not been allowing it out for anyone that is not participating in the Pilot. Only because we might change some stuff. The DOJ interim policy can be shared since it is available to the public.

From: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7)(C); (b)(7)(F) (b)(7)(F) (b)(7)(F) (b)(6); (b)(7)(C); (b)(7)(C); (b)(7)(F) (b)(6); (b)(7)(F) (b)(7

(b)(6); (b)(7)(C);

Is the BWC interim policy publicly available that we can provide it to agencies who are not part of the pilot and are thinking about implementing BWC's at their departments? Thanks in advance.

(b)(6); (b)(7)(C); (b)(7)(F)

United States Marshals Service Florida/Caribbean Regional Fugitive Task Force

(b)(6); (b)(7)(C); (b)(7)(F)

This information is for U.S. Marshals Service LIMITED OFFICIAL USE and is LAW ENFORCEMENT SENSITIVE. E-mails are protected under the Electronic Communications Privacy Act, 18 U.S.C. 119 Sections 2510, 2511, and 2521. Dissemination to non-law enforcement sources is strictly prohibited without prior approval. Any inquiries concerning this information should be directed to the sender of this email.

From: (b)(6): (USMS)

Sent: Fri, 3 Jan 2020 19:20:37 +0000

To: USMS-BWC; (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)(7)(F) USMS) (b)(6); (b)(7)(C); (b)(7)(F)

(USMS); (b)(6); (b)(7)(C); (USMS)

Cc: Kelly, Richard (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS); Tyler, Jeff (USMS)

Subject: RE: DOJ TFO BWC Pilot Program Update

Attachments: BWC MOU Addendum - Attachment B - 12.31.19.pdf, BWC DOJ Interim Policy -

Attachment A.PDF, BWC SOP FINAL 1.2.2020.pdf, BWC Checklist - Attachment C - 1.2.2020.pdf

All;

Here are the final BWC Pilot docs for your review and for sharing with your Pilot City partner agencies. Please let us know of any progress or obstacles in the execution of the required paperwork (other than those already noted in previous calls). Also, please keep your USAO POC updated as they are coordinating the process across all DOJ component agencies.

Being that we only just provided these docs for your review today, we will not have a call this afternoon to get your feedback. We will resume the Friday conference calls on January 10th. A meeting invite will be sent out with appropriate information.

Thanks.

Regards,

(b)(6); (b)(7)(C); (b)(7)(F)

Domestic Investigations Branch United States Marshals Service Mobile: (b)(6): (b)(7)(C)

From: (b)(6); (b)(7)(C); USMS)
Sent: Monday, December 30, 2019 3:30 PM
To: USMS-BWC@usdoj.gov; (b)(6); (b)(7)(C); (b)(7)(F) USMS (b)(6); (b)(7)(C); usms.doj.gov>; (b)(6); (b)(7)(C); (b)(7)(C); (b)(7)(C); (b)(7)(C); (b)(7)(C); (c)(7)(C);
(USMS) (b)(6); (b)(6); (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(6); (b)(6); (b)(6); (b)(6); (b)(7)(C);
(USMS) (b)(6); (b)(7)(C); pusms.doj.gov>
Cc: Kelly, Richard (USMS) (b)(6); (b)(7)(C) @usms.doj.gov>; (b)(6); (b)(7)(C); (b)(7)(F) USMS)
$\begin{array}{cccccccccccccccccccccccccccccccccccc$
Subject: DOJ TFO BWC Pilot Program Update

All;

We at HQ apologize for the lack of information flowing over the last couple weeks but with the holidays and some critical DOJ component level meetings to sort out revisions to the DOJ Interim Policy there has been no new information to provide.

Here are some updates on the status of the TFO BWC Pilot;

- DOJ has revised the Interim Policy and provided the updated policy to component agencies on Friday, December 27th
- DOJ has added Minneapolis/St. Paul as a pilot city as of Saturday, December 28th
- IOD is revising the MOU BWC Addendum to reflect the changes in the DOJ Interim Policy
- IOD is finalizing the BWC Pilot SOP to reflect the changes in the DOJ Interim Policy
- ITD has secured demo/training services through AXON and is pursuing funding for full services that can support the pilot period

We expect to have all updated documents to you by Thursday January 2^{nd} and hope to re-convene the Friday afternoon conference calls on January 3^{rd} .

Thank you for bearing with us as we continue to work through the complex issues at the Department and Agency levels.

2021-USMS-362780 118 2nd Interim Response

Have a safe New Year's holiday!

Regards,

(b)(6); (b)(7)(C); (b)(7)(F)

Domestic Investigations Branch
United States Marshals Service
Mobile (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C); (USMS) From: Sent: Tue, 17 Mar 2020 21:10:26 +0000 (b)(6); To: (USMS) (b)(6); (b)(7)(C); (b)(7)(F) (USMS) Cc: (USMS) RE: VRS - 2 page Walk-Thru Subject: Attachments: TFO BWC Pilot Axon Walkthrough Guide_ 3.12.20.docx (b)(6); (b)(7)(C) This is the most current version. I can make any changes on this tonight or tomorrow if you'd like. We're pretty much in shut down mode here in E/MO. I'll have plenty of time to help out with anything remotely if you need it. (b)(6); (b)(7)(C); (b)(7)(F) Eastern District of MO - St. Louis 111 South 10th Street, St. Louis MO, 63102 (b)(6); (b)(7)(C) -Cell (USMS) From: Sent: Tuesday, March 17, 2020 2:10 PM **To:** (b)(6); (b)(7)(C); $(USMS)^{(b)(6); (b)(7)(C);}$ usms.doj.gov> Cc: (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); (b)usms.doj.gov>; (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); usms.doj.gov> Subject: VRS - 2 page Walk-Thru (b)(6); Where did we leave off with the 2 page walk through? I sent something back last Thursday or Friday and was looking to finalize this week. Goal is to send the 1 page Quick Reference Guide to the program, the full VRS User Manual and the 2 page VRS Walk-Thru to the pilot city offices this week for their review. We just need to get our material reviewed by ITD and OGC before they are "official". Thanks. Regards, (b)(6); (b)(7)(C); Domestic Investigations Branch United States Marshals Service Mobile: (b)(6); (b)(7)(C)

Page 120

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 121

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

of the Freedom of Information and Privacy Act

From:	Tyler, Jeff (USMS)
Sent:	Fri, 15 Nov 2019 21:18:05 +0000
To:	Jankowski, Mark (USMS); (b)(6); (b)(7)(C); USMS); Blankinship, Gary (USMS);
Williams, Johnny (USN	(USMS); O'Keefe, Donald (USMS); Gonzales, David (USM); (b)(6); (b)(7)(C); (b)
(b)(6); (b)(7)(C); (USMS); Harr	ris, Matthew (USMS), (b)(6); (b)(7)(C); (USMS); Miller, Ronald (USMS); Beam, Craig
(USMS)	
Cc:	Kelly, Richard (USMS); (b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); (b)(7)(F) (USMS);
(b)(6); (b)(7)(C); (b)(7)(F) USN	MS); (b)(6); (b)(7)(C); (DSMS)
Subject:	Task Force Addendum
Attachments:	BWC MOU Addendum - rev. 11-2019.pdf
All	
	participation. Attached is the addendum as discussed. Please let us know if you
have any questions.	
Regards	
1-66	
Jeff	
Joffroy P. Tylor Assi	stant Director Investigative Operations Division
	te Washington, DC 20530-0001
(b)(6); (b)(7)(C) Offi	ice (b)(6); (b)(7)(C) Cell

From: (b)(6); (b)(7)(C); (USMS)

Sent: Tue, 26 Nov 2019 19:09:30 +0000

To: <u>USMS-BW</u>C

Cc: (b)(6); (b)(7)(C); (b)(7)(C); (b)(7)(F) (USMS); Kelly, Richard (USMS); (b)(6); (b)(7)(C); (b)(7)(F)

(USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(

(b)(6); (USMS)

Subject: USMS BWC Pilot City Group

Attachments: BWC Partner Agency Checklist 11.25.19 - FINAL.docx

Importance: High

All;

Thank you for your investment of time and patience as we work though the DOJ initiated Body Worn Camera pilot program at both the field and HQ levels. We know this is a difficult scenario to navigate with our pilot city partner agencies. IOD, OGC and ITD have been very much involved in the DOJ component level calls from the start and wanted to be able to share information directly with this group. We felt establishing this email group would facilitate communication, especially in light of the lack of conference calls over this shortened holiday week. This group contains the USMs and CDUSMs for all pilot city Districts and the relevant OGC, ITD and IOD personnel.

For everyone's benefit, please see the below priority items being worked on at the HQ level;

- IOD is coordinating the finalization of the necessary draft documents to proceed with the BWC Pilot in the designated cities.
 - MOU BWC Pilot Addendum (finalized and previously shared)
 - Partner Agency BWC Checklist/Survey (finalized and attached)
 - USMS Standard Operating Procedures for BWC Pilot (pending)
 - Video Retention Service (pending)
- ITD is working closely with a vendor (Axon) for a cloud based solution for storage and access
 - O POC for all technical aspects is (b)(6); (b)(7)(C); (b)(7)(F)

 (b)(6); (b)(7)(C); @usms.doj.gov
 - OGC and IOD are providing guidance on legal and operational aspects
 - o Demonstrations and training are being sought as part of this process

The Partner Agency BWC Checklist is attached. It is a survey for your Pilot City partner agencies to complete that will provide critical information on policies, procedures and technical details essential to establishing a viable means to share and secure BWC recordings related to USMS mission activity.

I hope that through this email group we will be able to provide you with more consistent updates on this pilot program process.

Please let me know if there are additional personnel that would be appropriate to include in this email group.

Thanks.

Regards,

(b)(6); (b)(7)(C); (b)(7)(F)

Domestic Investigations Branch
United States Marshals Service
Mobile: (b)(6); (b)(7)(C)

PARTNER AGENCY BODY WORN CAMERA CHECKLIST

Each Partner Agency requiring its United States Marshals Service (USMS) deputized personnel to wear Body Worn Cameras (BWC) on a USMS-led task force must complete this checklist prior to any Task Force Officer (TFO) being able to wear and deploy his/her BWC. Attach additional sheets if necessary.

To be filled out by USMS:

USMS Task Force Point of Contact (POC)				
Division/District (Role)	Name	Phone Number	Email Address	

To be filled out by each Partner Agency/Organization:

Ge	ographical Area Covered:	(area covered agency)	
BWC Program Role BWC POC Phone Email			Email
Policy/Program			
Technical			
Legal			
	Participating Agency TF	O's Information	
Name	Title/Rank	Phone	Email

^{**}Please insert rows to this if needed**

1. Identify legal authority or policies specific to the Partner Agency Organization, including any legal requirements related to post-video production access or use (e.g., FOIA, etc.):

1.A. State and Local Legal Authority List and attach any state or local laws applicable to BWCs or impacting BWCs (e.g., open records laws, legal retention requirements, ordinances, etc.); and other pertinent legal guidance (e.g., significant case law, State AG Opinions, etc.). If none, enter "N/A." Add additional rows as necessary.				
#	Title	Citation	Comments	
1				
2				

Law Enforcement Sensitive//For Official Use Only

1.B. Partner Agency Policies List and attach any policy, procedure, or other written directive from the Partner Agency applicable to TFOs' use of BWCs. Include any union or other labor agreement requirements regarding BWCs applicable to TFOs. If none, enter "N/A." Add additional rows as necessary.				
#	Title	Policy/Citation	Comments	
1				
2				

- 2. Provide information relevant to the Video and Body Worn Camera required to be used on a USMS task force operation. There are four related parts:
 - A. BWC System Information May require organizational technical staff coordination
 - B. BWC Use and Activation
 - C. Law Enforcement Access to BWC Recordings
 - D. External Access to BWC Recordings

	2.A. BWC System Information				
Aı	Answer the following questions, including any applicable citation or reference (e.g., state or local				
	law, agency policy, vendor contract, etc.).				
1	Name/model of BWC used by Partner Agency?				
	How are the Partner Agency's software licenses				
	structured?				
	Attach technical specifications if deviates from				
	USMS technical specifications. The USMS technical				
	specifications can be found in the Video Retention				
	System attachment.				
2	Note if there is internal organizational storage of				
	recordings or external storage with a third party				
	vendor? If a third party is present, identify the				
	vendor, the system, and attach the contract.				
3	Provide technical POC information used for systems				
	support. Provide Partner Agency operational service				
	desk support telephone number to be used for BWC				
	technical issue resolution.				
4	Provide technical information on the default				
	systems' governance related to data storage,				
	metadata captured, time interval default settings,				
	and back-up/archival frequencies and settings.				
	How long will recordings be preserved in the Partner				
	Agency's system? Attach any Partner Agency				
	retention schedule and note whether it is mandated				
	by state/local law or agency policy only. Include				
	external agency systems where the data may also				
	reside.				

2.A. BWC System Information Answer the following questions, including any applicable citation or reference (e.g., state or local law, agency policy, vendor contract, etc.).			
5	Does the BWC system include a "buffer"/ "pre- record" function or a "post-record" function? If either, identify and state the length of the buffer/pre-record and/or post-record, and whether it is audio only or both audio and video.		
6	Does the system allow redaction? How are redacted copies managed? Is the system tied to any other systems for automated work flow (e.g., eDiscovery, FOIA, etc.) or export production?		
7	What options exist to export video/metadata to external media and through which external media type (e.g., secure web link, Blue Ray, Thumb drive, etc.)?		
8	Does the system have an option available to allow the TFO or Partner Agency to upload or share the recordings and associated data to a USMS authorized system through a secure web interface? Are there any specialized requirements to allow access by designated USMS personnel to view and copy TFO recordings once uploaded? If there are any specialized software or interconnection requirements, please provide.		
9	Does the BWC system allow restriction of BWC recording access to specific persons within the Partner Agency?		
10	Does the system have an audit function that will identify persons who accessed, downloaded, altered or copied recordings? Can the system export audit logs on TFO cases to be shared with USMS?		
11	How will USMS cases be identified in the Partner Agency's system? How will the system append the USMS required metadata to the files? What metadata can be obtained from and added to BWC recordings?		
12	How does the Partner Agency handle inadvertent/accidental recordings?		
13	How does the Partner Agency handle requests to delete BWC recordings? How does the Partner Agency handle national security or sensitive material deletions? How does the Partner Agency handle unauthorized recordings? (Unauthorized recordings are considered those using specialized or sensitive investigative techniques, operating in a		

Ar	2.A. BWC System Infornswer the following questions, including any applicable law, agency policy, vendor co	citation or reference (e.g., state or local
	sensitive area, or working in an undercover or covert status on behalf of the federal task force).	
14	Confirm the TFO BWC user will be able to upload the recordings into the USMS BWC system. Can this be done locally at the USMS Task Force Office or is it only available at the Partner Agency site? How will this upload and data share be completed by the TFO or Partner Agency?	
15	What are the Video Codec and Video formats used for the video content? What are the quality settings on the BWC capture device? What is the frame rate of exported data? Is a predefined watermark enabled?	
16	Does the BWC have a GPS function? If so, is the function available to the TFO or embedded in the BWC function during video capture? What is the Partner Agency's policy regarding use of GPS? Can it be deactivated on TFO BWCs? If active, provide additional information on the configuration (including bread crumb intervals) and how that additional data can be shared with the USMS as part of the TFO BWC or Partner Agency upload to the USMS authorized system.	
17	Does the BWC have a "live stream" capability? If so, is the function available to the TFO? What is the Partner Agency's policy regarding use of "live streaming" with BWCs? Can it be deactivated on TFO BWCs? Can it be shared in real time with USMS? If different from standard TFO BWC recordings, provide information on metadata, storage, archival procedures, and access related to live stream data.	
18	Does the Partner Agency utilize facial recognition technology with BWC recordings? How? What metadata is maintained in support of the facial recognition and can it be disabled?	
19	Does the Partner Agency provide the TFO BWC officer with technical training on the use and sharing of recordings?	
20	Does the Partner Agency have predefined roles with specific settings or user configurable options based on those roles? How are those roles and settings configured?	

2.A. BWC System Information Answer the following questions, including any applicable citation or reference (e.g., state or local law, agency policy, vendor contract, etc.). 21 Provide a Partner Agency POC who can provide information regarding system security and protections, and location and security precautions of data storage facilities. *Do not attach this information it will be requested at a later time.*

	2.B BWC Use and Activation			
	Answer the following questions, including any applicable citation or reference (e.g., state or			
	local law, agency policy, vendor contract, etc.).			
1	Are there any exceptions under the TFO BWC			
	Partner Agency policy to the requirement to			
	record search warrant executions or arrests?			
2	What is the Partner Agency's policy regarding			
	BWC recording of confidential informants,			
	sources, and witnesses?			
3	Does the Partner Agency prohibit BWC			
	recording in any specific situations or			
	authorized exceptions? If so, list.			
4	Under the Partner Agency policy, are there			
	circumstances when a supervisor may direct			
	the officer to record or not record?			
5	What is the Partner Agency's policy regarding			
	citizen notification of BWC recording?			
6	How is the Partner Agency planning to meet			
	the DOJ requirement for allowing use only			
	during: (1) a planned attempt to serve an			
	arrest warrant or other planned arrest; or (2)			
	the execution of a search warrant?			
7	How will the Partner Agency meet the DOJ			
	requirement to prevent recording prohibited			
	content for the following: (1) undercover			
	personnel; (2) confidential informants or			
	confidential sources; (3) on-scene witness			
	interviews prior to or after the operation; (4)			
	personnel using specialized or sensitive			
	investigative techniques or equipment; or (5)			
	actions by any non-law enforcement persons at			
	the scene who are assisting law enforcement			
	personnel as determined by the federal agency			
	sponsoring the task force.			
8	If the TFO's BWC is inoperable, does the			
	Partner Agency's policy permit the TFO to			
	participate in enforcement activities if a			
	replacement is not readily available?			

	Answer the following questions, including a	Access to BWC Recordings ny applicable citation or reference (e.g., state or cy, vendor contract, etc.).
1	Are officers allowed to review BWC	
	recordings before writing reports or before	
	giving statements or testimony? If so, are	
	they allowed to view recordings only from	
	their own BWC, or are they allowed to view	
	BWC recordings from other officers?	
2	If officers are allowed to review recordings,	
	are there any exceptions? If so, list the	
	exceptions (e.g., internal investigations,	
	critical incidents, etc.).	
3	Who in the Partner Agency will have access	
	to TFOs' BWC recordings involving	
	USMS/federal cases? Who in other Federal	
	Agencies is allowed access to the recordings?	
	How are those access lists and permissions	
	maintained? What is the frequency at which	
	access is validated? How is access controlled	
	following access termination?	
4	Does the Partner Agency restrict access to	
	BWC recordings involving a critical incident	
	(e.g., officer-involved shootings, etc.)? If so,	
	who has access in those situations? How are	
	the restriction controls managed?	
5	Can the Partner Agency identify BWC	
	recordings on USMS cases by specific	
	metadata and limit access to those	
	recordings in the BWC system?	
6	Does the Partner Agency require random or	
	directed supervisory review/audit of officer	
	videos for policy compliance or other issues?	
	If so, will this include TFO recordings of USMS	
	cases?	
7	Will non-law enforcement employees of the	
	Partner Agency or municipality have access	
	to USMS BWC recordings (e.g., IT or local	
	government officials)? If so, are they CJIS-	
	compliant (e.g., CJIS background checks)?	2-1

	2.C. Law Enforcement Access to BWC Recordings Answer the following questions, including any applicable citation or reference (e.g., state or local law, agency policy, vendor contract, etc.).			
8	Are TFO BWC officers allowed to make copies	, , , , , , , , , , , , , , , , , , , ,		
_	of BWC recordings, or must they obtain			
	recordings from someone else within the			
	Partner Agency? Are officers allowed to			
	share and upload copies to the USMS			
	authorized systems or does the Partner			
	Agency require involvement?	24		
9	Are officers or other Partner Agency			
	employees allowed to retain copies of			
	recordings outside the police facility or retain			
	possession of copies for personal use?			
10	Does the Partner Agency have a policy			
	prohibiting sharing of recordings outside of			
	law enforcement for non-official reasons?	- 4		
11	Does the Partner Agency have a policy			
	prohibiting the posting of BWC recordings to			
	the Internet, social media sites, or the media	i/A		
	for non-official purposes?			
12	Does the Partner Agency have a policy			
	prohibiting officers from wearing or using			
	privately owned BWCs or any other non-			
	Partner Agency-issued BWC?			
13	Do any other law enforcement entities or			
	personnel have direct access to recordings			
	(e.g., a prosecutor's office, etc.)?			
14	Does the Partner Agency allow access to			
	redacted materials? If so, please explain.			
15	How does the Partner Agency ensure TFOs			
	understand the access and content			
	restriction policy requirements? Is there			
	training? What is the frequency?			
16	Does the Partner Agency investigate their			
	TFO-involved shootings (or other events			
	involving death or serious injury), or is this			
	done by another agency? If another agency:			
	Identify the agency.	M		
	Is there an agreement, policy, or protocol			
	in place with the agency for handling			
	these situations? If so, attach.			
	Are related archived records handled			
	differently than the standard processes?			
	If so, how?			

	2.D External Acces	s to BWC Recordings
		y applicable citation or reference (e.g., state or
		y, vendor contract, etc.).
1	 How does the Partner Agency handle external requests for BWC recordings? Criminal discovery, subpoenas? Civil/administrative discovery, subpoenas? Open record/FOIA requests? Media requests? Union requests? Is there an agreement with the union regarding union disclosure of BWC recordings? If so, attach copy. Local government authority requests? Civilian review board requests? Other? Are there any policies, local laws, or 	
	requirements related to release?	
2	 If the Partner Agency uses a third party vendor to store recordings: Is security of or access to recordings addressed in the contract? Are background checks of vendor employees addressed in the contract? Is the system CJIS compliant? Is access of content by the systems support technicians restricted? If so, how? If so, attach copy. 	
3	How does the Partner Agency handle redaction of BWC recordings prior to public release?	
4	How does the Partner Agency handle PII and sensitive content during a release? If any legal statements or content markings are included with release, please provide.	
5	Are there time-based or access restrictions on how long the external data may be maintained or used upon release? Are there any additional notifications required? If released, does the Partner Agency maintain a record copy longer than the standard policy for retention? If so, what is the deviation from that policy?	
6	How does the Partner Agency handle the approval request process and notifications of release?	

(b)(6); (b)(7)(C); (USMS) From: Sent: Mon, 2 Mar 2020 21:22:54 +0000 $(USMS)_{\underbrace{(b)(6); (b)(7)(C);}_{(b)(7)(F)}} (USMS); \underbrace{(b)(6); (b)(7)(C);}_{(b)(7)(F)}$ (USMS); (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); To: (b)(6); (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS) USMS) Subject: Body Worn Camera QRG Attachments: TFO BWC Pilot-QRG_2.26.20.pdf × Please see the attached for the finalized Quick Reference Guide (QRG) for the Body Worn Camera pilot program. Thank you, (b)(6); (b)(7)(C); (b)(7)(F)

(b)(6); (b)(7)(C) -Cell

Task Force Officer Body Worn Camera Pilot

QUICK REFERENCE GUIDE

Applies To:

- Specially Deputized Task Force Officers (TFOs) who are mandated by their parent
 agency to wear Body Worn Cameras (BWC) while assigned to a United States Marshals
 Service (USMS) Task Force.
- A Violent Offender Task Force memorandum of understanding BWC Addendum must be executed by the parent agency prior to a TFO deploying a BWC on USMS missions.
- Notification must be made to IOD of any request to execute a BWC Addendum prior to deployment of a TFO with a BWC on a USMS mission.

Recordings:

- TFOs may activate their parent agency-issued BWCs for the purpose of recording their actions ONLY during:
 - o A planned attempt to serve an arrest warrant or other planned arrest; or
 - The execution of a search warrant.
- TFOs are authorized to activate their BWCs upon approaching a premises or upon approaching a subject.
- TFOs must deactivate their BWCs when the scene is secured.
- TFOs shall verbally notify Task Force participants when activating BWCs during an operation and will advise when BWCs are deactivated, when feasible.
- TFOs may not use BWCs outside of the geographic area covered by their parent agency.
- TFOs are prohibited from recording:

(If recorded, it must be noted in Axon for awareness and potential redaction purposes)

- Undercover personnel
- Confidential informants or sources
- o On-scene witness interviews prior to or after the operation
- Personnel using specialized investigative techniques or equipment
- Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel
- If using specialized or sensitive investigative techniques
- o If operating in a sensitive area or is working in an undercover or covert status
- TFO BWC recordings can only be disseminated outside a parent agency in accordance with the Department of Justice Interim Policy on the use of BWC by Federally Deputized Task Force Officers, which includes approval from the USMS Office of General Counsel.

Reportable Incidents: (Urgent or specific situations fully or partially recorded by TFO BWC)

- Reportable Incidents include the following (contact IOD-DIB):
 - Shooting incident
 - Any incident which involves serious bodily injury or death resulting from any enforcement action by USMS personnel including use of force or deadly force
 - o Physical assault or attempted physical assault on a law enforcement officer
 - Intentional damage to a USMS facility, USMS conveyance, or other USMS property.

REV. 2/24/2020

From: (b)(6); (USMS)

Sent: Fri, 3 Jan 2020 00:03:47 +0000

To: (b)(6); (b)(7)(C); (b)(7)(F) USMS); Kelly, Richard (USMS); (b)(6); (b)(7)(C); (USMS);

(b)(6); (b)(7)(C); (b)(7)(F) (USMS)

Cc: (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); (b)(7)(F) USMS); Tyler, Jeff (USMS)

Subject: BWC Docs for Pilot Cities

Attachments: BWC Checklist – Attachment C 1.2.2020.pdf, FINAL BWC MOU Addendum - Rev.

12.31.19.pdf, BWC DOJ Policy (Revised Final).pdf, BWC SOP FINAL 1.2.2020.pdf

Importance: High

All;

Please see the attached finalized docs in PDF. These will be sent to the Pilot City offices tomorrow by noon, unless there are last minute issues that need addressed. All comments and concerns have been addressed or were deemed as not requiring changes and have been deleted.

Note: The DOJ Interim Policy doc will be fixed and have the inadvertent text boxes removed.

Thanks.

Regards,

(b)(6); (b)(7)(C); (b)(7)(F)

Domestic Investigations Branch United States Marshals Service

Mobile: (b)(6): (b)(7)(C)



UNITED STATES MARSHALS SERVICE (USMS)

Investigative Operations Division Domestic Investigations Branch

Body Worn Cameras
Standard Operating Procedures
Version 1.0
January 2, 2020

Signatures and Approval

Process Owner	
(Signature)	(Date)
(b)(6); (b)(7)(C); (b)(7)(F) Domestic Investigations Branch Investigative Operations Division	
Process Approver	
(Signature)	(Date)
Jeffrey R. Tyler Assistant Director Investigative Operations Division	

Change Control

All SOP changes must be version controlled and archived. New/major revisions will be indicated by a X.0. (1.0, 2.0, etc.) format. Maintenance/minor revisions will follow a 1.a format (e.g., 1.0.a, 1.0.b, etc.).

Version #	Approver	Approval Date	Change Details
1.0	Jeffrey R. Tyler January 2020	New SOP	

Table of Contents

I.	Purpose	1
II.	Authority	1
III.	Scope	1
IV.	Roles and Responsibilities	1
٧.	Operational Procedures	2
VI.	Technical Procedures	5
VII.	Reporting	8
VIII.	Training	9
IX.	Definitions	10
X.	Acronyms	10
XI.	Cancellation	11
XII.	Attachment	11

Purpose: The following guidelines set forth the procedures within the United States Marshals Service (USMS) for the operational use of Body Worn Cameras (BWCs) by specially-deputized USMS task force personnel and the collection, retention, documentation, and dissemination of digital media created by such equipment use. USMS managers and supervisors are responsible for ensuring that the United States Department of Justice (DOJ) Interim Policy – Use of Body-Worn Cameras by Federally Deputized Task Force Officers (hereinafter, "DOJ Interim BWC Policy"), the respective Task Force Memorandum of Understanding (and BWC Addendum), and other applicable DOJ and USMS policies and procedures, to include those outlined herein, are followed when BWCs are utilized during USMS fugitive and other criminal investigations.

The USMS regularly partners with state, local and tribal law enforcement agencies throughout the nation on USMS-led joint task forces. These relationships are vitally important to the USMS and its mission to protect our communities. Several of these participating state and local agencies have adopted internal policies mandating the use of BWCs and have requested that their officers wear BWCs while conducting planned arrests and searches during federal task force operations. To the extent state and local law enforcement agencies mandate BWCs for Task Force Officers (TFOs) while engaged in USMS task force operations, DOJ, through the DOJ Interim BWC Policy, has authorized such federally deputized TFOs from those agencies to use their BWCs under circumstances specified in that policy. The use of BWCs pursuant to the DOJ Interim BWC Policy, the USMS Task Force Memoranda of Understanding (MOU) (and an associated BWC-related Addendum), and this SOP do not replace the requirement to provide thorough written documentation of an incident. All data, images, video and metadata captured, recorded, or otherwise produced, is subject to federal law regarding retention of federal records and is the property of the United States Government and the USMS.

- II. Authority: This SOP is issued under the authority of the Assistant Director (AD), Investigative Operations Division (IOD), and the DOJ Interim BWC Policy.
- III. Scope: IOD is responsible for the establishment and implementation of all policy and procedures relating to BWCs used by USMS TFOs pursuant to the DOJ Interim BWC Policy and the USMS BWC Addendum to the Task Force MOU. These policies and procedures include, but are not limited to, the operational use by, and training of, USMS TFOs that utilize BWCs while in support of a USMS-led Fugitive Task Force; procurement (retention systems only); and the collection, retention, documentation, dissemination, and disposition of records relating to BWC use by TFOs. This SOP applies to all USMS personnel, specially-deputized federal, state, local or tribal officers working with the USMS in our enforcement operations and USMS contractors.

IOD and the USMS Office of the General Counsel (OGC) are responsible for Agency-wide oversight to ensure compliance with the DOJ and USMS BWC policies and these procedures, as well as other applicable federal and state law, DOJ and USMS policies, procedures, and regulations, to include, but not limited to, those relating to record-keeping and USMS records dissemination. District and Regional Task Force Chief Deputies and Commanders are responsible for the daily management of BWCs worn by TFOs in their respective districts and regions as specified within the DOJ Interim BWC Policy, and herein.

IV. Roles and Responsibilities

A. The AD, IOD, will be responsible for managing and overseeing the USMS BWC Program as well as implementing the DOJ Interim BWC Policy. This SOP promotes compliance with its provisions; ensures that use of BWCs by TFOs during regional and district task force operations receive the required approvals in accordance with the referenced policies and this SOP; and ensures USMS personnel, TFOs, contractors, and participating task force partners operate in accordance with applicable laws, regulations, rules, policies, and procedures. This SOP will also ensure compliance with those rules and regulations that control the collection, retention,

- documentation, dissemination, and disposition of records, to include those that contain personal identifying information (PII) collected by BWCs. IOD is the chief administrative component of the USMS BWC Program and shall ensure compliance with program policies and regulations and applicable federal, state, and local laws. IOD is responsible for establishing and maintaining operational policies and procedures associated with all USMS TFO BWC use.
- B. The United States Marshal (USM) and Chief Deputy United States Marshal (CDUSM) will be responsible for the overall supervision and management of any BWC Program within their district. In those areas where there is an IOD Regional Fugitive Task Force (RFTF), the Commander will be responsible for the overall supervision and management of the BWC Program related to those state and local law enforcement agencies where there is a task force MOU and BWC Addendum in place. The CDUSM/Commander is responsible for ensuring that the district or regional BWC Program complies with the policies and procedures outlined in the DOJ and USMS BWC policies and these SOPs. The CDUSM/Commander is also responsible for ensuring USMS personnel, TFOs, and contractors are aware of their responsibilities to protect sensitive law enforcement capabilities, limitations, and procedures and that they understand relevant legal and policy parameters associated with the USMS BWC Program, including the DOJ and USMS BWC policies and this SOP.
- C. The Information Technology Division (ITD) will be responsible for identifying, implementing, and maintaining an appropriate Video Retention System (USMS-VRS) for BWCs, in coordination with IOD and OGC. The AD, ITD, will be responsible for the overall supervision and management of the USMS-VRS, to include meeting all security requirements for the retention of recorded video or metadata and identifying technical specifications.
- D. USMS OGC provides legal guidance to the USMS BWC Program to ensure its compliance with applicable laws, regulations, policies and procedures; reviews and processes all requests for USMS testimony or disclosures of information including, but not limited to, in state and federal courts, regarding the USMS BWC Program, to ensure, inter alia, the security of sensitive investigative techniques and USMS privileged information; reviews and processes all Freedom of Information Act (FOIA) and Privacy Act requests regarding the USMS BWC Program, in direct consultation with IOD, and/or designees; and reviews and consults with the USMS Office of Congressional and Public Affairs (OCPA) on all congressional and press inquiries relating to BWCs. Through its FOIA/Privacy Officer, OGC also assesses the potential intrusiveness associated with BWC usage on privacy and civil liberties, balanced against the relevant governmental interests, and where appropriate, makes recommendations consistent with applicable privacy and civil liberty protections and follows existing procedures to review, investigate, and address privacy and civil liberties complaints.
- E. OCPA reviews and handles all congressional and press inquiries relating to the USMS BWC Program, in coordination with IOD, OGC, the relevant task force leadership, and any relevant components. The District and Division components are prohibited from responding to state, local, tribal, or territorial government authorities, on any aspects of the USMS BWC Program without coordinating with OCPA, IOD, and OGC.
- F. To ensure BWC usage is consistent with the DOJ Interim BWC Policy, the RFTF Commander and/or District CDUSM must document in writing TFO Parent Agency and TFO review and acknowledgment of said policies and SOPs prior to BWC utilization. TFO Parent Agency review and acknowledgment will be accomplished through the execution of an Addendum to the existing Task Force MOU. Individual TFO acknowledgment will be accomplished through an initialed copy of said policies and SOPs being placed in the applicable Regional Task Force Field Office or District Field Office.

V. Operational Procedures

A. Use of Body Worn Cameras:

Page 2

- 1. BWCs may only be utilized by TFOs assigned to USMS task forces, and then only if required by their parent agency and subject to the DOJ and USMS BWC policies and this SOP. USMS personnel and contractors are not authorized to wear or use BWCs.
- 2. Task Force participating agencies must have an executed Violent Offender Task Force (VOTF) or RFTF MOU, as well as the BWC Addendum and the Partner Agency Checklist, prior to the TFOs utilizing BWCs during USMS task force operations. If the Partner Agency fails to comply with any part of the DOJ policy, the MOU and Addendum, and this SOP, the relationship established under the MOU may be immediately terminated.
- 3. Unless subject to a specific exception below, TFOs employed by a law enforcement agency that mandates the use of BWCs on a USMS Task Force may wear and activate their recording equipment for the purpose of recording their actions ONLY during:
 - a. A planned attempt to serve an arrest warrant or other planned arrest; or
 - b. The execution of a search warrant.
- 4. TFOs are authorized to activate their BWCs upon approaching a premises or upon approaching a subject, and must deactivate their BWCs when the scene is secured as determined by the USMS Task Force supervisor or team leader on the scene.
 - **a.** For purposes of these BWC policies, SOPs, and the MOU/Addendum, the term "secured" means that the scene is safe and under law enforcement control.
 - b. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement officer.
- 5. TFOs may not use BWCs outside of the geographic area covered by their parent agency.
- 6. TFOs may use only parent agency-issued and parent agency-owned BWCs. TFOs will not be allowed to possess or use any privately-owned BWC or other recording device of any kind.
- 7. In the event a TFO's BWC is not working or is inoperable due to a technical problem or cannot be used due to physical damage, the TFO may participate in the operation without using a BWC if consistent with the parent agency policy.
- **8.** Even when BWC use would be permissible in the circumstances set forth above, TFOs are prohibited from recording:
 - Undercover personnel;
 - **b.** Confidential informants or confidential sources;
 - c. On-scene witness interviews prior to or after the operation;
 - Personnel using specialized investigative techniques or equipment; or
 - e. Actions by any non-law enforcement persons at the scene who are assisting law enforcement personnel.
- 9. Even when BWC use would be permissible in the circumstances set forth in Section V.A.3. above, TFOs are prohibited from activating their BWC if, in the judgment of the USMS Task Force supervisor or team leader, the TFO:
 - a. Is using specialized or sensitive investigative techniques;
 - **b.** Is operating in a sensitive area; or
 - c. Is working in an undercover or covert status on behalf of the USMS task force or the USMS.

2021-USMS-362780 141 2nd Interim Response

- 10. Even when BWC use would be permissible in the circumstances set forth in Section V.A.4 above, TFOs shall not use BWCs to record any activities related to:
 - National Security (including international and domestic terrorism investigations or cases involving classified information);
 - **b.** Public Corruption;
 - c. Medical Facilities; or
 - d. Other sensitive investigations as determined by USMS.
- 11. To the extent the TFO BWC is activated by these specialized functions to include, but not limited to, photographic capabilities, automatic recording synched to sensors or other initiating factors, such as vehicle light bar activation, taser removal, gun removal, stealth mode activation, etc., the BWC use is only permissible in the circumstances set forth in Section V.A.3 above.
- 12. The DOJ Interim BWC Policy of permitting the limited use of BWCs on task forces does not apply to highly specialized or sensitive operations or groups as determined by the USMS Task Force.
- **13.** When feasible, TFOs shall verbally notify Task Force participants when activating BWCs during an operation, and likewise will advise when BWCs are deactivated.
- **14.** TFOs are prohibited from using or activating BWCs within USMS work space. This includes any USMS-operated facility, training site, or USMS-controlled area.
- B. Partner Agency Internal Controls:
 - For purposes of the DOJ Interim BWC Policy, this SOP, and the MOU Addendum, the term "TFO BWC recordings" refers to audio and video recordings, and associated metadata, from TFO BWCs made while the TFO is working under federal authority, including state and local warrants adopted by the USMS.
 - 2. The Partner Agency will provide and maintain a central point-of-contact (POC) for the USMS on BWC matters.
 - 3. Access to any recording produced through TFO utilization of BWCs during USMS operations must be limited by the TFO Parent Agency to only personnel in the direct supervisory chain-of-command of the TFO or other administrative personnel necessary to the retrieval of the BWC footage.
 - 4. The Partner Agency will notify the USMS of any change in state or local law that will modify how TFOs must use BWCs and recordings.
 - 5. The Partner Agency will notify the USMS prior to making any change in agency policy that will affect the MOU Addendum or the storage, transfer, or redaction of TFO BWC recordings.
 - **6.** The Partner Agency will provide specifications to USMS personnel on the BWCs capabilities and operation.
 - 7. The Partner Agency will restrict access to any TFO BWC GPS and/or live stream capability as required by the USMS as determined by the local USM, CDUSM, or RFTF Task Force Commander.
- C. Handling of TFO BWC Recordings Made During USMS Task Force Operations:
 - 1. All TFO BWC recordings made during USMS task force operations, including such recordings retained by the Partner Agency and/or in the possession of any third party engaged by the Partner Agency to store or process BWC recordings, shall be deemed federal records of the DOJ/USMS pursuant to the Federal Records Act, meaning they are

- controlled by, and the property of, DOJ/USMS and cannot be disseminated without the written permission of DOJ/USMS.
- 2. The Partner Agency will provide full, un-redacted copies of TFO BWC recordings to the USMS for all activations that record data of USMS task force related operations. The existence of TFO BWC recordings must be reported in the USMS authorized record system.
- 3. As a federal record, the Partner Agency will restrict access to TFO BWC recordings within the Partner Agency. The Partner Agency is authorized to use TFO BWC recordings for internal investigations of its personnel consistent with the parent agency's policies and procedures, not involving dissemination outside the parent agency or public release. The parent agency shall provide written notification to the sponsoring federal agency prior to any internal review.
- 4. The Partner Agency will notify USMS immediately of any unauthorized access to TFO recordings discovered by the agency. The Partner Agency will cooperate fully with the USMS in the investigation of any unauthorized access to or disclosure of TFO BWC recordings, including providing USMS the name(s) of any Partner Agency personnel determined by the agency to be involved in unauthorized access, copying, or disclosure.
- In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings, and as potential evidence in a federal investigation subject to applicable federal laws, rules, and policy concerning disclosure or dissemination; and therefore deemed privileged absent appropriate redaction prior to disclosure or dissemination.
- 6. If a TFO BWC recording involves a "reportable incident" as defined below, or involves another time-sensitive or urgent situation, the Partner Agency will provide the USMS access to copies on an expedited basis, including during non-business hours. For purposes of this provision, "reportable incident" means:
 - a. Shooting incident
 - **b.** Any incident which involves serious bodily injury or death resulting from any enforcement action by USMS personnel including use of force or deadly force;
 - c. Physical assault or attempted physical assault on a Law Enforcement Officer;
 - **d.** Intentional damage to a USMS facility or USMS conveyance.
- 7. The Partner Agency will provide witnesses, as needed, to authenticate TFO recordings in USMS cases.
- 8. The Partner Agency will inform USMS of the length of time TFO BWC recordings will be retained by the agency before deletion.
- 9. The Partner Agency will notify USMS as soon as possible regarding any request or demand for release or disclosure of TFO BWC recordings, and refer the request to USMS.
- 10. The Partner Agency will not publicly release TFO BWC recordings without the express, written permission of USMS. The Partner Agency will not release or disseminate TFO BWC recordings to any other law enforcement agency, to any state or local prosecutor, or any other entity without the express written permission of USMS.
- 11. The Partner Agency will redact any video or audio portion of TFO BWC recordings when requested by the USMS, to the extent the Partner Agency has the necessary redaction capability.

VI. Technical Procedures

A. The USMS has developed a cloud-based USMS-VRS to provide technical capabilities to assist in post-operational management of content captured by TFO BWCs to meet requirements set forth within the DOJ Interim BWC Policy, as well as the USMS BWC policy and this SOP.

B. Technical Specifications

- The USMS will maintain classification of data types for appropriate record keeping management functions. Data types include, but are not limited to, Evidence, Non-Evidence, Legal, FOIA, and Records Management.
- 2. TFO BWC recordings shall meet the minimum technical specifications required for federal Information Technology (IT) compliance and USMS-VRS system interoperability. Specifications and USMS application framework will be provided in the Partner Agency Checklist. Quality, format, codec, timestamp, and external reference time will need to meet federal IT compliance requirements.
- 3. Critical technical elements which will impact metadata validation of TFO BWC recording organization and management include:
 - Standard user-identity naming convention for accounts with a valid associated email account.
 - b. Metadata, which shall be included by the Partner Agency prior to sharing or uploading TFO BWC recordings to the authorized USMS-VRS. Metadata tags will be required, must be validated, and will allow for additional, optional tags from the local level Task Force POC.
 - c. The proper categorization of TFO BWC recordings to ensure proper chain of custody and safeguard against unauthorized deletion of content. TFO BWC recordings may come in varied formats and can be loaded and aligned with the TFO BWC recordings which are part of the case file related to the arrest activity. Examples of categories include video, administrative data (pictures, files, etc.), TFO notifications, and metadata entries. All video content must be associated with the USMS-related Federal Identification Number (FID).
- 4. The USMS-VRS organizational structure will be defined by the AD, IOD in coordination with District/Division leadership, OGC, and ITD, for authorized levels as part of the standard governance framework to account for operational and administrative management access/options. The structure may also include a framework in support of internal sharing, supervisory review, reporting, content management, and group management.

C. Process

- 1. The AD, IOD, or their designee, will work with the Partner Agency POC to establish the ability for video collaboration with Partner Agency TFOs.
- 2. The Partner Agency will test video content sharing or upload capabilities and processes with validation of success from the CDUSM/Commander. The aforementioned technical specifications must be validated to ensure compliance with USMS policy.
- 3. The CDUSM/Commander will ensure the shared link, third party video upload notification, and instructions are sufficient for Partner Agency uploads for TFO BWC recordings through an external secure link. The CDUSM/Commander is responsible for ensuring TFOs who wear BWCs understand both the shared and upload process requirements related to coordinated delivery of Partner Agency TFO BWC recordings. Critical elements or information related to sensitive content may be required to be added if missing at the time of receipt validation or if critical to the management of TFO BWC recording records.
- **4.** The CDUSM/Commander will validate receipt of compliant video content in the USMS-VRS, note any internal data content anomalies as required, and track and audit content.

2021-USMS-362780 144 2nd Interim Response

D. Basic USMS-VRS Capabilities (USMS.Evidence.
--

- USMS Task Force Officer User or TFO Parent Agency User Sign-In
 - a. To sign in to Evidence.com, you must go to your Partner Agency's Evidence.com page from a web browser, then go to the USMS's unique URL:

(b)(7)(E)

- b. In the Username and Password boxes, type the appropriate information, which will be provided by the USMS IT Program Coordinator, and select sign-in.
- c. Evidence.com may require a security response validation and may send you an email with a code to ensure authorized access. Note that if you sign in to Evidence.com while you are already signed in from another location, your original session will be terminated.

2. Dashboard Content Awareness

a. The Dashboard will appear once you sign in to Evidence.com. You can also return to the Dashboard page from any other area in Evidence.com by clicking the Axon logo in the upper-left corner of the page. The Dashboard includes sections used to manage the capabilities for the CDUSM/Commander, USMS IT Program Coordinator, or other administrative activities.

3. Critical Device Alerts

The USMS-VRS will send alerts via email to notify the USMS about activity in the system related to USMS cases, to include evidence management, upcoming evidence deletions, case management, account management, external video uploads, and USMS-VRS performance and system usage.

4. Case Management

- a. Case management will allow the USMS to organize related evidence files, such as files that pertain to the same incident. Users can share videos with other authorized users via a download link. Collaborative video content sharing is for operational purposes and is controlled by the USMS.
- b. An enclave for TFO BWC recording storage, which will be accessible through a web browser with a standard organizational framework, will be established to aid in proper case management. Files in the enclave shall not be shared without authorization.

5. Partner Agency Access

6.

- a. The USMS will establish ties between the approved Partner Agency and Axon services for the TFO BWC submitters and the CDUSM/Commander users to share content.
- b. An Administrator at the USMS will add selected agencies to allow for a partner option.
- c. The Partner Agency must first accept the USMS invitation, then enable TFOs' ability to have access to upload to the the USMS agency and share data with a specific USMS deputy.

Metada	ıta		
a.			
		(b)(7)(E)	

		(b)(7)(E)	
land			
Video Collaboration (Canabilitiaa		
Video Collaboration (Japabilities		
		(b)(7)(E)	
		, , , , , ,	

c. For both Axon and third party video content, bulk tagging, sharing, and upload options are available.

VII. Reporting

- A. Recorded Video or Metadata:
 - Collection and retention of data, images, video, or metadata during the deployment of a BWC will adhere to the procedures set forth herein and <u>USMS Policy Directive 8.13</u>, <u>Evidence</u>, where applicable.

2021-USMS-362780 146 2nd Interim Response

2.		
	(b)(7)(E)	

- 3. The USMS shall not retain information collected using BWC that may contain personally identifiable information (PII) for more than 120 days, unless the retention of information is determined necessary for an authorized purpose. Authorized purposes may include, but are not limited to, law enforcement investigations and litigation. Data collected by BWC that is retained must be placed in the appropriate video retention system and safeguarded in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and other guidance. These authorities ensure that DOJ personnel with access to such data follow practices that are consistent with the protection of privacy and civil liberties. Use of all DOJ information systems, which may include BWC component parts, may be monitored, recorded, and subjected to audit.
- **4.** BWC recordings not retained for authorized purposes may only be deleted upon approval from the Task Force Supervisor, IOD, and OGC.
- **5.** When data, images, video, or metadata are stored in the authorized USMS-VRS, the following must be recorded:

(b)(7)(E)

- 6. Data, images, video, and metadata shall not be shared for any purpose (to include law enforcement sharing requests) outside the USMS without permission first from the USMS IOD, OGC and, if and as appropriate, the Office of Public Affairs, the Training Division, IOD/Office Operational Technologies, and the relevant U.S. Attorney's Office. IOD and OGC will engage in and coordinate any expeditious review to the extent required by the DOJ Interim BWC Policy. This is because any data, image, video recording, or metadata obtained through BWC activity is a federal record, subject to FOIA, 5 U.S.C. § 552. All requests for such information from third parties must be directed to the USMS FOIA Office. Further, information sharing relating to the use of BWC may be restricted by DOJ and USMS policies, procedures, laws and regulations governing the disclosure of federal information and records, to include the DOJ Touhy Regulations, 28 C.F.R. § 16.21 et seq. In addition, such information and records may be subject to various privileges restricting or prohibiting their disclosure.
- 7. Prior to any TFO utilization of BWCs, the applicable TFO Partner Agency must provide the USMS with written documentation describing the Partner Agency's retention policy of the BWC recordings, and owner/contractor which is providing BWC equipment, instruction, and data storage to the TFO Partner Agency. Please refer to the Partner Agency Checklist for further information.

VIII. Training

- A. All USMS personnel, TFOs, and contractors associated with a USMS task force must be familiar with the DOJ Interim BWC Policy, all sections of the BWC Addendum to the VOTF/RFTF MOU, and these procedures.
- **B.** USMS personnel will be required to instruct all TFOs that utilize BWCs during USMS operations on how to utilize the appropriate video retention system utilized by the USMS and log BWC use in the USMS records management system (JDIS).

IX. Definitions:

- **A.** Body Worn Cameras (BWC): Small cameras, which can be clipped onto a police officer's uniform or worn as a headset and turned on to record video and audio of law enforcement encounters with the public.
- **B.** Task Force Officers (TFOs): Federal, State, Local, and Tribal Law Enforcement Officers who are specially deputized by the USMS and participate in USMS-led enforcement operations.
- C. Metadata: A set of data that describes and gives information about other data.
- **D.** Personal Identifying Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, that is linked or linkable to a specific individual.

X. Acronyms:

- A. AD: Assistant Director
- B. BWC: Body Worn Cameras
- C. CDUSM: Chief Deputy United States Marshal
- D. DOJ: Department of Justice
- E. FID: Federal Identification number
- F. FOIA: Freedom of Information Act
- G. GMT: Greenwich Mean Time
- H. GPS: Global Positioning System
- I. IOD: Investigative Operations Division
- J. ITD: Information Technology Division
- K. MOU: Memorandum of Understanding
- L. NIST: National Institute of Standards and Technology
- M. OCPA: Office of Congressional and Public Affairs
- N. OGC: Office of General Counsel
- PII: Personally Identifying Information
- P. POC: Point of Contact
- Q. RFTF: Regional Fugitive Task Force
- R. SOP: Standard Operating Procedure
- S. TFO: Task Force Officer
- T. USM: United States Marshal
- U. USMS: United States Marshals Service
- V. USMS-VRS: United States Marshals Service Video Retention System

W. UTC: Coordinated Universal Time

X. VOTF: Violent Offender Task Force

Y. VRS: Video Retention System

XI. References:

A. USMS Policy Directive 8.13, Evidence

XII. Cancellation: Supersedes prior interim guidance.

XIII. Attachment(s):

- A. DOJ Interim BWC Policy
- B. BWC Addendum
- C. Partner Agency Checklist

Tyler, Jeff (USMS) From: Sent: Mon, 23 Dec 2019 18:22:33 +0000 (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS): USMS); To: (b)(6); (b)(7)(C); (b)(7)(F) (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (b)(6); (USMS); (USMS); (b)(6); (b)(7)(C); (b)(7)(F) (USMS) Cc: Kelly, Richard (USMS) Subject: **BWC FINAL DRAFT for approval-Kelly** Attachments: BWC FINAL DRAFT for approval-Kelly.docx All Outstanding job putting together this comprehensive SOP. Rich and I combined our comments into this single document. Please address as appropriate and send back so we can finalize. If you have any questions please let me know. **Thanks** Jeff

Jeffrey R. Tyler, Assistant Director | Investigative Operations Division

(b)(6); (b)(7)(C)

U.S. Marshals Service | Washington, DC 20530-0001

Office |

(b)(6); (b)(7)(C)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

Withheld pursuant to exemption

(b)(5) Deliberative Process Privilege ; (b)(7)(E)

(USMS) From: Sent: Tue, 29 Oct 2019 21:22:38 +0000 (USMS); (b)(6); (b)(7)(C); (USMS); (b)(6); (b)(7)(C); (b)(7)(F) To: (b)(6); (b)(7)(C); (b)(7)(F) (b)(6); (b)(7)(C); USMS) USMS) (b)(6); (b)(7)(C); (b)(7)(F Cc: USMS) FW: BWC Announcement Subject: Attachments: BWC DOJ Policy (Final).pdf

All;

See below and attached shared earlier today with the USMS leadership in the pilot cities.

From: Hackmaster, Nelson (USMS)
Sent: Tuesday, October 29, 2019 3:49 PM
To: Jankowski, Mark (USMS) (b)(6): (b)(7)(C) @usms.doj.gov>; Abdullah, Joe (USMS)
(b)(6); (b)(7)(C) @usms.doj.gov>; Blankinship, Gary (USMS) (b)(6); (b)(7)(C) @usms.doj.gov>; Williams, Johnny
(USMS) (b)(6); (b)(7)(C) Pusms.doj.gov>; Bieber, Jay (USMS) (b)(6); (b)(6); (b)(7)(C) Pusms.doj.gov>; O'Keefe, Donald
(USMS) (b)(6); (b)(7)(C) (Dusms.doj.gov>; Gonzales, David (USM) (b)(6); (b)(7)(C) (Dusms.doj.gov>; Hughes,
Timothy (USMS) (b)(6); (b)(7)(C) usms.doj.gov>; Harris, Matthew (USMS)(b)(6); (b)(7)(C) usms.doj.gov>; Holt,
Brandon (USMS) (b)(6); Dusms.doj.gov>; Miller, Ronald (USMS) (b)(7)(C) (Dusms.doj.gov>; Beam, Craig
(USMS) (b)(6); Dusms.doj.gov>
Cc: Tyler, Jeff (USMS) (b)(6); usms.doj.gov>; Kelly, Richard (USMS) (b)(6); Dusms.doj.gov>; (b)(6);
(b)(6); (b)(7)(C); (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); (b)(7)
(USMS) (b)(6); pusms.doj.gov>; Wade, Drew J. (USMS) (b)(6); (b)(7)(C) pusms.doj.gov>; Delaney, William
(USMS) (b)(6); (b)(7)(C) @usms.doj.gov>; (b)(6); (b)(7)(C); (b)(7)(F) (USMS) (b)(6); (b)(7)(C); @usms.doj.gov>
Subject: BWC Announcement

Leadership,

Attached is the approved DOJ Interim Policy for the BWC Pilot Program. Please hold off sharing this with your effected state and local agencies until we can set up a conference call tomorrow afternoon and discuss further. The components are still hashing out a little granularity as we speak so that we apply this policy, and execute the pilot program consistently across all of DOJ. I anticipate that at the conclusion of our call tomorrow you will be free to share the policy and begin having those conversations with your state and local partners. To assist you with these conversations, IOD and OGC are developing talking points that they will share with you once finalized. As a reminder please reach out to OCPA for guidance on any media inquiries as this is likely to receive increasing attention. Thanks! R/Nelson

(b)(6); (b)(7)(C): will you please help us set up a conference line in 16064 for tomorrow at 4:00 pm est and respond to all with the number and passcode. Thanks!

Nelson Hackmaster Associate Director U.S. Marshals Service

(USMS) (b)(6); (b)(7)(C); (b)(7)(F) (b)(6); (b)(7)(C); (b)(7)(F) (USMS) From: Sent: Friday, August 27, 2021 2:41 PM Kelly, Richard (USMS); (b)(6); (b)(7)(C); To: (USMS) (b)(6); (b)(7)(C); (b)(7)(F) (USMS) Cc: Subject: FW: MOU Appendix USMS Fugitive Task Force MOU - CCSO Signature 8.27.21.pdf; USMS MOU Letter Attachments: 8.27.21 - Signed MOU Enclosed.pdf Follow Up Flag: Follow up Flagged Flag Status: As we have been able to be flexible and create the Appendix to the MOU Addendum, we're already seeing success in the partner agencies where concerns were noted. Cook County GLRFTF is a go! (b)(6); (b)(7)(C); (b)(7)(F) **USMS BWCPO** (b)(6); (b)(7)(C) (USMS) (b)(6); From: (b)(6); (b)(7)(C); @usms.doj.gov> Sent: Friday, August 27, 2021 12:44 PM (b)(6); Pusms.doj.gov>; (b)(6); (b)(7)(C); (b)(6); (USMS (b)(6); (b)(7)(C); Pusms.doj.gov> Subject: FW: MOU Appendix Fyi! From: (b)(6); (b)(7)(C); (b)(7)(F) (Sheriff) (b)(6); (b)(7)(C); (b)(7)(F) Occsheriff.org> Sent: Friday, August 27, 2021 10:58 AM (b)(6); (b)(7)(C); (b)(7)(F); (b) (b)(6); (b)(7)(C); (b)(6); (b)(7)(C); (Sheriff) @ccsheriff.org>; (b)(6); (b)(7)(C); (Sheriff) (b)(6); (b)(7)(C); @ccsheriff.org> Cc: (b)(6); (b)(7)(C); (b)(7)(F)(USMS) (b)(6); (b)(7)(C); @usms.doj.gov>; (b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); usms.doj.gov>; (b)(6); (USMS) (b)(6); (b)(7)(C); pusms.doj.gov> Subject: RE: MOU Appendix Good morning, Please see attached, please return executed copies of the MOU and Addendum to me. Thanks again for working through this with us. Have a great weekend! (b)(6); (b)(7)(C); **Deputy General Counsel** Cook County Sheriff's Office (b)(6): (b)(7)(C) (b)(6); (b)(7)(C); Please note my email address has changed to @ccsheriff.org

(b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); (b)(7)(F) @usdoj.gov> Sent: Wednesday, August 25, 2021 2:26 PM To: (b)(6); (b)(7)(C); (Sheriff) (b)(6); (b)(7)(C); occsheriff.org>; (b)(6); (b)(7)(C); (b)(7)(F) (Sheriff) (b)(6); (b)(7)(C); (Sheriff) • (b)(6); (b)(7)(C); occsheriff.org> Cc: (b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); (b)(7)(F) @usdoj.gov>[(b)(6); (b)(7)(C); (USMS) (b)(6); (b)(7)(C); (b)(7)(F)@usdoj.gov>; USMS) (b)(6); (b)(7)(C); @usdoi.gov> Subject: RE: MOU Appendix

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Good afternoon,

Attached is the final version (Appendix). This is the one we will use moving forward. I want to thank each of you for prioritizing this endeavor and making it happen. I value our partnership and looking forward to future operations while utilizing the BWC. Once the addendum is signed we will begin the next step which is the checklist to ensure we are able to share the data seamlessly ...we are at the 10 yard line about to punch it in. thanks, (b)(6).

(b)(6); (b)(7)(C); (b)(7)(F)

U.S. Marshals Service

Great Lakes Regional Fugitive Task Force

Cell: (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C); (b)(7)(F) USMS)

Sent: Tuesday, August 24, 2021 3:15 PM

To: (b)(6); (b)(7)(C); @ccsheriff.org; (b)(6); (b)(7)(C); (b)(7)(F) @ccsheriff.org; (b)(6); (b)(7)(C); @ccsheriff.org

Cc: (b)(6); (b)(7)(C); @ccsheriff.org

(USMS) (b)(6); (b)(7)(C); @usms.doj.gov

Subject: FW: MOU Appendix

Good afternoon,

Thank you for taking the time this morning during the conference call, we have added an appendix (attached) for your review. We are confident this will resolve the issues we talked about. Please review and let us know what you think. If you have any questions don't hesitate to contact us.

Respectfully,

(b)(6); (b)(7)(C); (b)(7)(F)

U.S. Marshals Service

Great Lakes Regional Fugitive Task Force

Cell: (b)(6); (b)(7)(C)



SHERIFF THOMAS DART Cook County Sheriff's Office Richard J. Daley Center 50 Washington Street, Suite 704 Chicago, Illinois 60602

August 27, 2021

VIA Electronic Mail

(b)(6); (b)(7)(C); (b)(7)(F)

U.S. Marshals Service Great Lakes Regional Fugitive Task Force

RE: USMS Fugitive Task Force MOU - Body Worn Camera Addendum

Dear (b)(6); (b)(7)(C); (b)(7)(F)

Thank you so much for taking the time this week to discuss the partnership between the Cook County Sheriff's Office ("CCSO") and the US Marshall Service ("USMS"), and for developing the additional appendix. As requested, enclosed you will find the following:

- Executed Memorandum of Understanding between the CCSO and USMS (the "MOU");
- 2. Executed Addendum to the MOU concerning use of Body Worn Camera by Task Force Officers incorporating the enclosed Appendix A; and
- 3. Copy of the CCSO's Body Worn Camera Policy.

Per Appendix A which has been incorporated by reference into the Addendum of the MOU, the enclosed copy of the CCSO's Body Worn Camera Policy shall serve as notice of the requirements set forth in Illinois State Law governing activation of body-worn cameras by Task Force Officers under the CCSO's chain of command. Please return fully executed copies of the MOU and Addendum to me at (b)(6); (b)(7)(C); (b)(7)(F) (c)csheriff.org. Thank you for your continued partnership and please contact me with any questions or concerns.

Sincerely,

(b)(6); (b)(7)(C); (b)(7)(F)

Deputy General Counsel Cook County Sheriff

Enclosures

Addendum to Fugitive Task Force Memorandum of Understanding RE: Body-Worn Camera Use by Task Force Officers

This Addendum supplements the current Memorandum of Understanding (MOU) between the United States Marshals Service (USMS) and the

(Hereinafter referred to as "Partner Agency" or "TFO parent agency")

Pursuant to the "U.S. Department of Justice Policy – Use of Body-Worn Cameras by Federally Deputized Task Force Officers," dated October 29, 2020 (hereinafter referred to as "DOJ Policy"), the above named Partner Agency has advised the USMS that it will require its Specially Deputized Task Force Officers (TFO) assigned to the USMS Task Force to use bodyworn cameras (BWCs). This Addendum governs that use.

The parties hereby agree to the following:

- I. The Partner Agency and their TFOs will be advised of and adhere to the DOJ Policy, USMS's Standard Operating Procedures for Body-Worn Camera Program for Task Force Officers, and other applicable federal and USMS policies, procedures, regulations, and laws, including those relating to federal records retention and information access.
- II. The Partner Agency confirms that prior to executing this agreement, it has provided to the USMS details regarding the BWC system and cameras, including the details of any system protections, and any state or local policies or laws applicable to the TFO's use of BWCs, including any retention policies, and training and access procedures.
- III. TFOs will follow the provisions set forth in this agreement for use of BWCs, and the provisions of this agreement will supersede any conflicting provision(s) in the Partner Agency's policy for TFOs while serving on the USMS Task Force.
- IV. Use of BWCs During USMS Task Force Operations:
 - A. TFOs may use only Partner Agency-issued and Partner Agency-owned BWCs.
 - B. TFOs will be allowed to wear and activate their BWCs for the purposes of recording their actions during USMS Task Force operations only during:
 - 1. A planned attempt to serve an arrest warrant or other planned arrest; or,
 - 2. The execution of a search warrant.

Page 1 of 6

- a. For the execution of a search warrant, BWCs should not be used for searches of property lawfully in government custody or control, or a search to obtain digital or electronic records executed by a third party, such as an electronic service provider or custodian of electronic records.
- C. TFOs are authorized to activate their BWCs upon approaching a subject or premises and must deactivate their BWCs when the scene is secured as determined by the USMS Task Force Supervisor or Team Leader on the scene.
 - 1. For purposes of this agreement, the term "secured" means the scene is safe and under law enforcement control.
 - 2. In the event circumstances arise requiring additional law enforcement assistance to secure the scene, the TFO will end BWC recording when relieved from the scene by another law enforcement officer.
- D. TFOs are authorized to wear and activate their recording equipment in accordance with the DOJ Policy anywhere they are authorized to act as a police or peace officer under state, local, territorial or tribal law.
- E. In the event a TFO's BWC is not working or is inoperable due to a technical problem or cannot be used due to physical damage, the TFO may participate in the operation without using a BWC if that continued participation is consistent with the Partner Agency policy.
- F. Even when BWC use would be permissible in the circumstances set forth in Section IV, subsection B, above, TFOs are prohibited from recording:
 - 1. Undercover personnel;
 - 2. Confidential informants or confidential sources;
 - 3. On-scene witness interviews prior to or after the operation;
 - 4. Personnel using specialized investigative techniques or equipment; or,
 - 5. On-scene actions by any non-law enforcement persons who are assisting law enforcement personnel prior to or after the operation.
- G. Even when BWC use would be permissible in the circumstances set forth above in Section IV, subsection B, TFOs are prohibited from activating their BWC if, as determined by the USMS, the TFO is:
 - 1. Using specialized or sensitive investigative techniques;
 - 2. Operating as part of a highly specialized or sensitive operation or group;

Page 2 of 6

- 3. Operating in a sensitive area; or
- Working in an undercover or covert status on behalf of the USMS Task Force or the USMS itself.
- H. Even when BWC use would be permissible in the circumstances set forth above in Section IV, subsection B, subject to the discretion of the USMS, TFOs generally shall not use BWCs to record any activities related to investigations involving:
 - Public Corruption;
 - 2. Medical Facilities;
 - 3. National Security (including international and domestic terrorism investigations or cases involving classified information); or
 - 4. Other sensitive investigations as determined by the USMS.

V. Partner Agency Internal Controls:

- A. For purposes of this agreement, the term "TFO BWC recordings" refers to audio and video recording(s), and associated metadata, from TFO BWCs made while the TFO is working under federal authority, including when executing state and local warrants adopted by the USMS.
- B. The Partner Agency will provide and maintain central points-of-contact (POC), at a minimum two POCs, a primary and secondary, for the USMS on BWC matters. The Partner Agency will notify the USMS of any change to the POCs.
- C. The Partner Agency will notify the USMS of any change in state or local law or policy that will modify how TFOs must use BWCs and handle recordings.
- D. The Partner Agency will notify the USMS prior to making any change in agency policy that will affect the MOU Addendum or the storage, transfer, or redaction of TFO BWC recordings.
- E. The Partner Agency will provide specifications to USMS personnel on the BWC capabilities and operation.
- F. If applicable, the Partner Agency will restrict access to any TFO BWC GPS and/or livestream capability as required by the USMS.
- VI. Handling of TFO BWC Recordings Made During USMS Task Force Operations:

Page 3 of 6

- A. All TFO BWC recordings made during USMS Task Force operations in accordance with this agreement, including recordings retained by the Partner Agency and/or in the possession of any third party engaged by the Partner Agency to store or process BWC recordings are federal records of the USMS and the United States Department of Justice pursuant to the Federal Records Act, and shall not be disseminated by the TFO, TFO Partner Agency, or any third party, as described here, without advance written notification to the USMS of their intention to do so as soon as practical. The parties consider this to be a limited waiver of the requirements under the Federal Records Act and Department of Justice regulations regarding records disclosure.
- B. The Partner Agency will provide full, un-redacted, duplicate copies of TFO BWC recordings to the USMS for all activations that record data of USMS Task Force-related operations. The existence of TFO BWC recordings relating to a USMS Task Force operation must be recorded in the USMS authorized record system. Additionally, an unredacted copy of any recording to be released by the TFO Partner Agency shall be provided to the USMS prior to said release.
- C. As a federal record, the Partner Agency will restrict access to TFO BWC recordings within the Partner Agency as provided in the Agency's internal policies. The Partner Agency is authorized to use TFO BWC recordings for internal review of its personnel consistent with the Partner Agency's policies and procedures but may not disseminate the BWC recording outside the Partner Agency or for public release without advance written notification to the USMS.
- D. The Partner Agency will notify the USMS immediately of any unauthorized access to TFO BWC recordings discovered by the Partner Agency. The Partner Agency will cooperate fully with the USMS in the investigation of any unauthorized access to or disclosure of TFO BWC recordings, including providing the USMS with the name(s) of any Partner Agency personnel determined by the Partner Agency to be involved in unauthorized access, copying, or disclosure.
- E. In all circumstances, TFO BWC recordings shall be treated as law enforcement sensitive information. The premature disclosure of these recordings could reasonably be expected to interfere with enforcement proceedings and may be potential evidence in a federal investigation subject to applicable federal laws, rules, and policy concerning disclosure or dissemination and therefore are deemed privileged, absent appropriate redaction prior to disclosure or dissemination. Further, BWC recordings may be entirely exempt from public release or other disclosure or dissemination under applicable federal and state laws, rules, and policy.
- F. If a TFO BWC recording involves a "reportable incident," as defined below, or involves another time-sensitive or urgent situation, the Partner Agency will provide the USMS access to copies on an expedited basis, including during non-business hours.
 - 1. For purposes of this provision, "reportable incident" means:

Page 4 of 6

- a. shooting incident;
- any incident which involves serious bodily injury, death, or where any enforcement action by USMS personnel resulted in the use of force or deadly force;
- physical assault or attempted physical assault on a Law Enforcement Officer;
 and.
- d. intentional damage to any facility, conveyance, or other property owned by USMS.
- G. The Partner Agency will provide witnesses, as needed, to authenticate TFO recordings in litigation.
- H. The Partner Agency will inform the USMS of the length of time TFO BWC recordings will be retained by the Partner Agency before deletion.
- I. The Partner Agency will notify the USMS in writing as soon as possible regarding any request or demand for release or disclosure of TFO BWC recordings. In all circumstances, TFO BWC recordings may only be disseminated in accordance with the requirements contained within this MOU addendum.
- J. Expedited Public Release: If TFO BWC recording(s) depict conduct committed solely by a TFO resulting in serious bodily injury or death of another, the TFO's Partner Agency shall notify the USMS as early as possible if it desires to publicly release the recording(s). Following the notification, the TFO's Partner Agency may immediately release the recording(s) with any redactions as appropriate, giving as much advance notice as possible to the USMS as to the time and manner of its release. The USMS will expeditiously review the recording(s) as soon as practical.

	(b)(7)(E)	

K. A USMS enforcement action or incident may require additional support from law enforcement officers with the Partner Agency. In the event those assisting law enforcement officers have BWCs, any captured video from those cameras will be made available by the Partner Agency to the USMS upon request.

- VII. The USMS will ensure that all USMS Task Force partner agencies are informed of which other partner agencies, if any, mandate BWC use by their respective TFOs and are authorized to have their TFOs wear BWCs on the USMS Task Force.
- VIII. If the Partner Agency fails to comply with any part of this Addendum, the relationship established under the Task Force Memorandum of Understanding may be immediately terminated.

Digital signatures are preferred

Name: Cook	County Sheriff's Office	Phone: 312-603-6444
Location (City an	ad State): Chicago, IL / Co	ook County, IL
	ENCY REPRESENTATIVE (b)(6); (b)(7)(C); (b)(7)(Title:	<u></u>
(t	o)(6); (b)(7)(C); (b)(7)(F)	8/27/2021 Date:
	RECTOR, INVESTIGATIO	ONS OPERATION DIVISION:
Signature:		Date:

Note: Signed Addendum MUST be submitted to the Investigative Operations Division with other required documentation to obtain authorization for participation in the TFO BWC Program prior to TFOs deploying with BWCs on USMS operations. The executed Addendum should be retained locally with the executed USMS Fugitive Task Force MOU.

Page 6 of 6



U.S. MARSHALS

Body-Worn Camera Program Office

TFO BWC MOU ADDENDUM

Appendix A

The following is additional guidance for situations that may be affect a task force partner agency regarding the TFO (Task Force Officer) BWC (Body-Worn Camera) MOU (Memorandum of Understanding) Addendum. This guidance is issued by the United States Marshals Service (USMS) Body-Worn Camera Program Office (BWCPO) and USMS Office of General Counsel (OGC):

- Review Boards/Other Public Dissemination: If an agency is under a consent decree or otherwise required by statute, law, or agreement to disclose BWC footage to a review board, that entity and their access to the agency BWC and the qualifying events or incidents that are the subject of the agreement will be described in a letterhead memo that the USMS will keep in the BWC MOU tracking system. The memo should include the timeline for that board to receive the footage, if their access to an agency BWC Video Retention System is direct or indirect, and whether the review board has independent/unilateral public disclosure authority. This information will assist the USMS OGC in determining what timeline they may be under to perform agency review if a qualifying incident occurs where TFO and/or USMS BWC footage has been recorded.
- State Law/Agency Policies: If state law or qualifying agency policy requires recording outside the parameters of USMS TFO BWC MOU Addendum, the agency will provide that information to the USMS BWCPO. The recordings of post-arrest events that are outside TFO enforcement action, i.e., medical facilities, prisoner transport, should be separated, if possible, by deactivation of the TFO BWC when the arrest scene is concluded and secure and reactivation when the officer is operating under his agency policy alone for a non-TFO agency responsibility. When separate recording(s) are possible, the USMS will receive only the enforcement BWC recording. If deactivation and reactivation are not feasible, the entire recording will be shared with USMS with the understanding that USMS will, if necessary, redact the entire portion of any recording that shows the TFO performing an agency duty where he is not operating under the USMS Task Force (TF) MOU parameters for enforcement actions.
- Short term operations: Any partner agency not covered by an existing executed USMS
 TFO BWC MOU Addendum and any non-partner TF agency are not authorized to utilize
 their BWC for any USMS operation they may join. This includes Operation
 Washout/Operation Triple Beam, national crime reduction initiatives, etc.

Law Enforcement Services Manual

Portable Audio/Video Recorders

520.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of the Cook County Sheriff's Office while in the performance of their duties (50 ILCS 706/10-20). Portable audio/video recording devices include all recording systems whether body-worn, handheld or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Cook County Sheriff's Office facility, authorized undercover operations, wiretaps, or eavesdropping (concealed listening devices).

520.1.1 ISSUANCE/EFFECTIVE DATE

This policy was re-issued on June 15, 2021 and shall become effective on July 1, 2021 at 0001 hours (statutory updates).

520.1.2 DEFINITIONS

Definitions related to and incorporated in this policy include those definitions contained in Section 10 of the Law Enforcement Officer-Worn Body Camera Act ("Body Camera Act") (50 ILCS 706/10-10):

Body-worn camera or camera (BWC) - An electronic camera system for creating, generating, sending, receiving, storing, displaying, and processing audio/visual recordings that may be worn about the person of a law enforcement officer.

Law enforcement-related encounters or activities - Activities in which the sworn member is enforcing the law, including traffic or pedestrian stops, arrests, searches, interrogations, investigations, pursuits, and crowd and traffic control. It does not include a community caretaking function, which is defined as a task undertaken by a sworn member in which the sworn member is performing an articulable act unrelated to the investigation of a crime. Community caretaking functions include, but are not limited to tasks unrelated to the investigation of a crime such as participating in town halls or other community outreach; helping a child find their parents; providing death notifications; performing in-home or hospital well-being checks on the sick, the elderly, or persons presumed missing; or completing paperwork while alone or only in the presence of another law enforcement officer.

Portable recorder or recorder - Either an audio-only recording device or a body-worn camera.

520.2 POLICY

The Cook County Sheriff's Office shall provide sworn members having the rank of Lieutenant and below access to portable recorders, either audio or video or both, for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Sheriff's Office by accurately capturing contacts between sworn members and the public.

Law Enforcement Services Manual

Portable Audio/Video Recorders

The use of body-worn cameras is specifically controlled by the Body Camera Act (50 ILCS 706 et seq.). Nothing in this policy related to body-worn cameras shall be construed to conflict with the Body Camera Act and where there is a conflict or ambiguity, the provisions of the Body Camera Act shall control.

520.3 MEMBER PRIVACY EXPECTATION

All recordings made by members on any department-issued device at any time, and any recording made while acting in an official capacity of the Sheriff's Office, regardless of ownership of the device it was made on, shall remain the property of the Sheriff's Office. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

Members should consider powering down the recorder when there is an expectation of personal privacy (e.g., the member using the restroom), ensuring the recorder is powered on again prior to returning to duty.

520.4 MEMBER RESPONSIBILITIES

If applicable, prior to going into service, each uniformed sworn member will be responsible for making sure that they are equipped with a portable recorder issued by the Sheriff's Office, and that the recorder is in good working order. If the recorder is not in working order or the sworn member becomes aware of a malfunction at any time, the member shall promptly report the failure to their supervisor and obtain a functioning device as soon as practicable (50 ILCS 706/10-20); see the respective Portable Audio/Video Recorders Procedure for further guidance. Uniformed sworn members should wear the recorder in a conspicuous manner and notify persons that they are being recorded, whenever possible.

Any sworn member assigned to a non-uniformed position, with approval of the respective department head or the authorized designee, may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed sworn members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever possible.

When using a portable recorder, the assigned sworn member shall record their name, star number and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Sworn members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording. Sworn members should include the reason for deactivation.

Law Enforcement Services Manual

Portable Audio/Video Recorders

520.5 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the portable recorder should be used, although there are many situations where its use is appropriate. Sworn members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

Sworn members wearing body-worn cameras and any clothing or other indication they are law enforcement shall have the body-worn camera turned on at all times while they are on-duty and are responding to calls for service or engaged in law enforcement-related activities (50 ILCS 706/10-20(a)(3)). Sworn members shall also have the body-worn camera turned on as otherwise required by policy, directed by training, or ordered by a supervisor.

Portable recorders, including body-worn cameras, should also be activated in any of the following situations:

- (a) All enforcement and investigative contacts, including stops and field interview situations.
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance, and all crime interdiction stops.
- (c) Self-initiated activity in which a sworn member would normally notify the Communications Center.
- (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.
- (e) Upon exiting a patrol vehicle for law-enforcement-related encounters (50 ILCS 706/10-20(a)(3)(B)), regardless of whether the vehicle is equipped with Mobile Audio/Video (MAV).
- (f) When the sworn member has reason to believe that the person on whose behalf the member is performing a community caretaking function has committed or is in the process of committing a crime. If exigent circumstances exist that prevent the camera from being turned on, the camera shall be turned on as soon as practicable (50 ILCS 706/20(a)(4.5)).

If exigent circumstances prevent a sworn member from turning on a body-worn camera when required, the camera shall be turned on as soon as practicable (50 ILCS 706/10-20(a)(3)(A)).

Sworn members shall not record interactions with confidential informants unless exigent circumstances exist or the informant has committed or is committing a crime (50 ILCS 706/10-20(a)(4)(C)).

Sworn members must provide notice of recording to any person if the person has a reasonable expectation of privacy and proof of notice must be evident in the recording. If exigent circumstances exist that prevent the sworn member from providing notice, notice must be provided as soon as practicable (50 ILCS 706/10-20(a)(5)).

Law Enforcement Services Manual

Portable Audio/Video Recorders

At no time is a sworn member expected to jeopardize their safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as practicable.

520.5.1 CESSATION OF RECORDING

Once activated, the portable recorder should continue to record until the sworn member's direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident (e.g., to conduct activity that is not relevant to the incident).

Body-worn cameras shall be turned off when a victim, witness, or community member reporting a crime requests that the camera be turned off. Unless impractical or impossible, the request should be captured on the recording (50 ILCS 706/10-20(a)(4)). However, a sworn member may continue to record or resume recording a victim, witness, or community member if exigent circumstances exist or the member has a reasonable articulable suspicion that the victim, witness, or community member has committed or is in the process of committing a crime. Under these circumstances, the sworn member should indicate on the recording the reason for continuing to record despite the request of the victim or witness (50 ILCS 706/10-20(a)(4)).

Sworn members are permitted to turn off body-worn cameras while inside a patrol vehicle equipped with MAV. Cameras may also be turned off when the sworn member is not engaged in law enforcement-related activities, when completing paperwork alone, when only in the presence of another law enforcement officer, or when the member is engaged in community caretaking functions (50 ILCS 706/10-10; 50 ILCS 706/10-20).

520.5.2 SURREPTITIOUS USE OF THE PORTABLE RECORDER

Sworn members may not surreptitiously record any conversation in which any party to the conversation has a reasonable belief that the conversation is private or confidential, unless otherwise authorized by law (720 ILCS 5/14-2).

However, sworn members using body-worn cameras are not prohibited from recording a person who has a reasonable expectation of a private conversation if the person is provided notice of the recording and proof of that notice is captured on the recording. If exigent circumstances exist that prevent the sworn member from providing notice, notice must be provided as soon as practicable (50 ILCS 706/10-20(a)(5)).

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the respective department head or the authorized designee.

520.5.3 EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

Law Enforcement Services Manual

Portable Audio/Video Recorders

520.6 PROHIBITED USE OF PORTABLE RECORDERS

Members are prohibited from using department-issued portable recorders and recording media for personal use, and they are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Except for authorized, legitimate department business purposes (i.e., related to official duties), members are also prohibited from retaining, duplicating or distributing recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. All such recordings shall be retained by the Sheriff's Office.

Members are prohibited from using personally owned recording devices while on-duty. Any member who uses a personally owned recorder for department-related activities (e.g., inadvertently makes a recording) shall comply with the provisions of this policy, including retention and release requirements, and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, intimidation, or ridicule.

520.7 IDENTIFICATION AND PRESERVATION OF RECORDINGS

Any time a sworn member records any portion of a contact that the member reasonably believes constitutes evidence in a criminal case, the member shall transfer the file in accordance with current procedure for storing digital files and document the existence of the recording in the related case report. Transfers should occur at the end of the sworn member's shift, or any time the storage capacity is nearing its limit.

To assist with identifying data and recordings, members should tag or mark these as needed in accordance with the respective Portable Audio/Video Recorders Procedure.

Any time a sworn member reasonably believes a recorded contact may be beneficial in a noncriminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

520.8 RETENTION OF RECORDINGS

All recordings other than those made with body-worn cameras shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days unless the recordings are made a part of an arrest or the recordings are deemed evidence in any criminal, civil, or administrative proceeding and then the recordings must only be destroyed upon a final disposition and an order from the court (720 ILCS 5/14-3(h-15)).

520.8.1 RETENTION REQUIREMENTS FOR BODY-WORN CAMERA RECORDINGS Recordings made on body-worn cameras shall be retained for 90 days. Recordings shall not be altered, erased, or destroyed prior to the expiration of the 90-day storage period (50 ILCS 706/10-20(a)(7)).

Law Enforcement Services Manual

Portable Audio/Video Recorders

In the event any recording made with a body-worn camera is altered, erased, or destroyed prior to the expiration of the 90-day storage period, the Sheriff's Office shall maintain, for a period of one year, a written record including:

- (a) The name of the individual who made such alteration, erasure, or destruction.
- (b) The reason for any such alteration, erasure, or destruction.

After the 90-day storage period, recordings must be destroyed unless any encounter captured on the recording has been flagged. An encounter is deemed flagged when any of the following occur (50 ILCS 706/10–20):

- (a) A formal or informal complaint has been filed.
- (b) The sworn member discharged their firearm or used force during the encounter.
- (c) Death or great bodily harm occurred to any person in the recording.
- (d) The encounter resulted in a detention or arrest, other than a traffic stop resulting in only a minor traffic offense or business offense (i.e., a petty offense with a fine of more than \$1,000) (50 ILCS 706/10-10).
- (e) The sworn member is the subject of an internal investigation or otherwise being investigated for possible misconduct.
- (f) The supervisor of the sworn member, prosecutor, defendant, or court determines that the encounter has evidentiary value in a criminal prosecution.
- (g) The recording sworn member requests that the video be retained for official purposes related to their official duties.

Under no circumstances shall any recording made with a body-worn camera relating to a flagged encounter be altered or destroyed prior to two years after the recording is flagged. If the flagged recording is used in a criminal, civil, or administrative proceeding, the recording shall not be destroyed except upon a final disposition and order from the court (50 ILCS 706/10-20(a)(7)(C)).

Following the 90-day storage period, recordings may be retained any time a supervisor designates the recording for training purposes and may be viewed by sworn members, in the presence of a supervisor or training instructor, for the purposes of instruction, training, or ensuring compliance with Sheriff's Office policies (50 ILCS 706/10-20(a)(8)).

520.8.2 RELEASE OF AUDIO/VIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

520.9 REVIEW OF RECORDED MEDIA FILES

Subject to the restrictions in the Video Access Prohibitions and Criminal Penalties subsection, the recording member and their supervisor may access and review recordings prior to completing incident reports or other documentation, provided that the member or their supervisor discloses that fact in the report or documentation (50 ILCS 706/10-20(a)(6)). Members shall not retain

Law Enforcement Services Manual

Portable Audio/Video Recorders

personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less-detailed report.

For the purposes of redaction, labeling, or duplicating recordings, access to camera recordings shall be restricted to only those members responsible for those purposes. The recording sworn member or their supervisor may not redact, label, duplicate or otherwise alter the recording member's camera recordings. The supervisor of the recording member may access and review recordings prior to completing incident reports or other documentation, provided that the supervisor discloses that fact in the report or documentation (50 ILCS 706/10-20(a)(6A)).

520.9.1 VIDEO ACCESS PROHIBITIONS AND CRIMINAL PENALTIES

Access restrictions - Sworn members shall not access or review their own video footage, or the body-worn camera recordings of another officer prior to completing an incident report when the member:

- (a) Has been involved in or is a witness to an officer-involved shooting, a use of deadly force incident, or a use of force incident resulting in great bodily harm or any apparent injury to a non-member; or
- (b) Is ordered to write a report in response to or during the investigation of a misconduct complaint against the sworn member.

For incidents with access restrictions, sworn members may file amendatory reports (e.g., supplemental reports) after viewing body-worn camera recordings. When doing so, the report shall contain documentation regarding access to the video footage (50 ILCS 706/10-20(a)(6)).

For a list of injuries that require medical assistance following a use of force, refer to the section entitled Medical Considerations in the Use of Force Policy.

Violators may be subject to a Class 3 felony (720 ILCS 5/33-9).

The recording member's assigned field training officer may access and review recordings for training purposes. Any detective or investigator directly involved in the investigation of a matter may access and review recordings which pertain to that investigation but may not have access to delete or alter such recordings (50 ILCS 706/10-20(a)(6B)).

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct, or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

- (a) Upon approval by a supervisor, or by any member of the Sheriff's Office who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.
- (b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.
- (c) By media personnel with permission of the respective department head or the authorized designee, in accordance with applicable laws and regulations.

Law Enforcement Services Manual

Portable Audio/Video Recorders

(d) In compliance with a public records request, if permitted, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed prior to public release (see the Records Maintenance and Release Policy) by the following:

- (a) The Custodian of Video Records (i.e., Video Monitoring Unit);
- (b) The Chief of Staff or the authorized designee;
- (c) The respective department head or the authorized designee;
- (d) The Executive Director of the Office of Public Relations or the authorized designee; and
- (e) The Sheriff's Legal Department General Counsel or the authorized designee.

Recordings that unreasonably violate a person's privacy or sense of dignity should not be publicly released unless disclosure is required by law or order of the court.

Access to recordings for redaction, labeling, or duplication shall be restricted to only those members responsible for those purposes (50 ILCS 706/10-20(a)(6)).

520.9.2 DOCUMENTING REVIEW OF RECORDINGS

Members who review recordings prior to completing incident reports or other documentation shall disclose that fact in the report or other documentation (50 ILCS 706/10-20(a)(6)).

520.9.3 REQUESTS FROM OUTSIDE AGENCIES OR INDIVIDUALS

No outside agency or individual requests for recordings (e.g., FOIA, subpoena) will be processed unless the request has been received by the Sheriff's Legal Department and approved by the Sheriff's General Counsel or the authorized designee.

520.10 BODY-WORN CAMERA COORDINATOR

The respective department head or the authorized designee should designate a coordinator responsible for the following (50 ILCS 706/10-20), including but not limited to:

- (a) Identifying members who are assigned body-worn cameras.
- (b) Identifying members permitted to access recordings in order to redact, label, or duplicate recordings.
- (c) Ensuring body-worn cameras acquired on or after July 1, 2015, are equipped with preevent recording of at least the 30 seconds prior to camera activation and are capable of recording for a period of at least 10 hours.
- (d) Establishing procedures for:
 - The care and maintenance of body-worn cameras, including reasonable efforts to be made by supervisors to correct or repair body-worn camera equipment upon notice from a member experiencing technical difficulties, failures, or problems with the equipment.

Law Enforcement Services Manual

Portable Audio/Video Recorders

- Compliance with the Law Enforcement Officer-Worn Body Camera Act and guidelines established by the Illinois Law Enforcement Training and Standards Board (ILETSB) for the use of body-worn cameras.
- Security of recordings including access controls.
- Redacting, labeling, and duplicating recordings.
- 5. Supervisor and member review of recordings.
- (e) Providing an annual report to the ILETSB pursuant to 50 ILCS 706/10-25.
- (f) Ensuring the Sheriff's Office uses authorized body-worn camera recording media (50 ILCS 706/10-10).

United States Marshals Service Fugitive Task Force Memorandum of Understanding

Rev. 11/2020

PARTIES AND AUTHORITY:

This Memorandum of Understanding (MOU) is entered into by the

Cook County Sheriff's Office

and the United States Marshals Service (USMS) pursuant to 28 U.S.C. § 566(e)(1)(B). As set forth in the Presidential Threat Protection Act of 2000 and directed by the Attorney General, the USMS has been granted authority to direct and coordinate permanent Regional Fugitive Task Forces consisting of Federal, state, and local law enforcement authorities for the purpose of locating and apprehending fugitives. The authority of the USMS to investigate fugitive matters as directed by the Attorney General is set forth in 28 USC § 566. The Director's authority to direct and supervise all activities of the USMS is set forth in 28 USC § 561(g) and 28 CFR 0.111. The authority of United States Marshals and Deputy U.S. Marshals, "in executing the laws of the United States within a State . . . [to] exercise the same powers which a sheriff of the State may exercise in executing the laws thereof" is set forth in 28 USC § 564. Additional authority is derived from 18 USC § 3053 and Office of Investigative Agency Policies Resolutions 2 & 15. (See also) "Memorandum for Howard M. Shapiro, General Counsel, Federal Bureau of Investigation" concerning the "Authority to Pursue Non-Federal Fugitives", issued by the U.S. Department of Justice (DOJ), Office of Legal Counsel, dated February 21, 1995. (See also) Memorandum concerning the Authority to Pursue Non-Federal Fugitives, issued by the USMS Office of General Counsel, dated May, 1, 1995. (See also) 42 U.S.C. § 16941(a)(the Attorney General shall use the resources of federal law enforcement, including the United States Marshals Service, to assist jurisdictions in locating and apprehending sex offenders who violate sex offender registration requirements).

MISSION: The primary mission of the task force is to investigate and arrest, as part of joint law enforcement operations, persons who have active state and federal warrants for their arrest. The intent of the joint effort is to investigate and apprehend local, state and federal fugitives, thereby improving public safety and reducing violent crime. Each participating agency agrees to refer cases for investigation by the RFTF (Regional Fugitive Task Force) or VOTF (Violent Offender Task Force). Cases will be adopted by the RFTF/VOTF at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy. Targeted crimes will primarily include violent crimes against persons, weapons offenses, felony drug offenses, failure to register as a sex offender, and crimes committed by subjects who have a criminal history involving violent crimes, felony drug offenses, and/or weapons offenses. Upon receipt of a written request, the RFTF/VOTF may also assist non-participating law enforcement agencies in investigating, locating and arresting their fugitives. Task force personnel will be assigned federal, state, and local fugitive cases for investigation. Investigative teams will consist of personnel from different agencies whenever possible. Participating agencies retain responsibility for the cases they refer to the RFTF/VOTF. Federal fugitive cases referred to the task force for investigation by any participating agency will be entered into the National Crime Information Center (NCIC) by the USMS or originating agency, as appropriate. State or local fugitive cases will be entered into NCIC (and other applicable state or local lookout systems) as appropriate by the concerned state or local agency.

SUPERVISION: The RFTF/VOTF will consist of law enforcement and administrative personnel from federal, state, and local law enforcement agencies. Agency personnel must be approved by the RFTF/VOTF Chief Inspector/Chief Deputy prior to assignment to the RFTF/VOTF. Agency personnel may be removed at any time at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy. Direction and coordination of the RFTF/VOTF shall be the responsibility of the USMS RFTF/VOTF Chief Inspector/Chief Deputy. Administrative matters which are internal to the participating agencies remain the responsibility of the respective agencies. Furthermore, each agency retains responsibility for the conduct of its personnel. A Task Force Advisory Committee, consisting of representatives of participating agencies and USMS RFTF/VOTF personnel, may be established at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy and will meet and confer as necessary to review and address issues concerning operational matters within the RFTF/VOTF.

PERSONNEL: In accordance with Homeland Security Presidential Directive 12, personnel assigned to the task force are required to undergo background investigations in order to be provided unescorted access to USMS offices, records, and computer systems. The USMS shall bear the costs associated with those investigations. Non-USMS law enforcement officers assigned to the task force will be deputized as Special Deputy U.S. Marshals. Task force personnel may be required to travel outside of the jurisdiction to which they are normally assigned in furtherance of task force operations. State or local task force officers (TFOs) traveling on official business at the direction of the USMS shall be reimbursed directly by the USMS for their travel expenses in accordance with applicable federal laws, rules, and regulations.

REIMBURSEMENT: If the Marshals Service receives Asset Forfeiture funding for either 1) overtime incurred by state and local investigators who provide full time support to USMS RFTF/VOTF joint law enforcement task forces; or 2) travel, training, purchase or lease of police vehicles, fuel, supplies or equipment for state and local investigators in direct support of state and local

Page 1 of 3 Rev. 11/2020

investigators, the USMS shall, pending availability of funds, reimburse your organization for expenses incurred, depending on which category of funding is provided. Reimbursement of overtime work shall be consistent with the Fair Labor Standards Act. Annual overtime for each state or local law enforcement officer is capped at the equivalent of 25% of a GS-1811-12, Step 1, of the general pay scale for the Rest of United States. Reimbursement for all types of qualified expenses shall be contingent upon availability of funds and the submission of a proper request for reimbursement which shall be submitted quarterly on a fiscal year basis, and which provides the names of the investigators who incurred overtime for the RFTF/VOTF during the quarter; the number of overtime hours incurred, the hourly regular and overtime rates in effect for each investigator, and the total quarterly cost. The request for reimbursement must be submitted to the RFTF/VOTF Chief Inspector/Chief Deputy, who will review the request for reimbursement, stamp and sign indicating that services were received and that the request for reimbursement is approved for payment. Supporting documentation must accompany requests for reimbursement for equipment, supplies, training, fuel, and vehicle leases.

VEHICLES: Pending the availability of asset forfeiture funding, the USMS may acquire vehicles to be utilized by state and local investigators assigned to the RFTF/VOTF. Vehicles provided by the USMS remain in the control of the USMS and must be used solely in support of RFTF/VOTF operations. The vehicles must be available for exclusive use of the TFOs assigned to the RFTF/VOTF by the undersigned participant agency for the duration of the agency's participation on the task force. If the agency is no longer a participating member of the RFTF/VOTF, any USMS vehicle provided to the agency for use by TFO(s) must be returned to the USMS. Operators of USMS-provided vehicles must adhere to USMS policy regarding the use of government owned vehicles. Any violation of the USMS vehicle policy may result in the vehicle being repossessed by the USMS and the operator and/or agency forfeiting the opportunity to utilize a USMS-provided vehicle in the future. Vehicles provided to state and local investigators may be subject to additional regulations or restrictions pursuant to USMS lease agreements. Replacement or removal of any vehicle provided by the USMS will be at the discretion of the USMS and/or subject to lease agreement terms.

EQUIPMENT: Pending the availability of Asset Forfeiture funding, the USMS may purchase equipment for state and local investigators assigned to the RFTF/VOTF. Equipment purchased by the USMS using Asset Forfeiture funding must be used solely in support of RFTF/VOTF operations. The equipment must be available for exclusive use of the TFOs assigned to the RFTF/VOTF by the undersigned participant agency for the duration of the agency's participation on the task force. If the agency is no longer a participating member of the RFTF/VOTF, any equipment purchased with Asset Forfeiture and provided to TFOs from the agency may be retained by the agency. Equipment provided by the USMS that is not purchased using Asset Forfeiture funding remains the property of the USMS and will be issued to state and local investigators for exclusive use in support of the RFTF/VOTF. If the investigator or agency is no longer a participating member of the RFTF/VOTF, any equipment issued that was not purchased with Asset Forfeiture funding will be returned to the USMS.

BODY-WORN CAMERAS AND TASK FORCE OFFICERS: As per DOJ Policy dated October, 29, 2020, Body Worn Cameras (BWC) may be worn by TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force. A partner agency must formally request to participate in the TFO BWC program and, upon approval, comply with all DOJ and USMS policies, procedures, documentation, and reporting during their participation. Moreover, pursuant to the DOJ BWC Policy, the USMS will inform all partner agencies of which other partner agencies, if any, have been authorized to have their TFOs wear BWCs on the Task Force, and provide all partner agencies with a copy of the DOJ BWC Policy. That information will be provided separately. Accordingly, all partner agencies should be aware that TFOs may be participating in the TFO BWC program and may be operating with BWCs on USMS task force operations in their agency's jurisdiction. TFOs whose parent agency is not approved for participation in the TFO BWC program are not allowed to deploy with BWCs on USMS missions.

RECORDS AND REPORTS: After the RFTF/VOTF has adopted a warrant, all investigative reports, evidence, and other materials generated, seized or collected by the RFTF/VOTF, relating to the fugitive investigation, shall be material within the custody and control of the RFTF/VOTF. Physical evidence, such as drugs, firearms, counterfeit credit cards, and related items may be released to the appropriate prosecuting agency. Records and information obtained during the RFTF/VOTF fugitive investigation are not evidence and may not be released. A participating agency may retain copies of RFTF/VOTF investigative reports, and other documents or materials, but they may be released only upon approval of the USMS Office of General Counsel, in consultation with the local U.S. Attorney's Office, if and as applicable.

All investigative reporting will be prepared in compliance with existing USMS policy and procedures utilizing USMS case management systems. Every effort should be made to document investigative activities on USMS forms, such as USM-11s and USM-210s. Reports should never contain information related to sensitive USMS programs that are deemed privileged and not subject to reporting. RFTF/VOTF records and documents, including reports on RFTF/VOTF activity prepared in cases assigned to TFOs, will be maintained in USMS electronic records. Task force statistics will be maintained in the USMS case management systems. Statistics will be made available to any participating agency upon request. This section does not preclude the necessity of individual TFOs completing forms required by their employing agency. However, reports documenting task force related investigations or activities prepared by a TFO on their parent agency form and any TFO's task force related email or text exchanges are deemed federal records under the control and purview of USMS, regardless of where these records are generated or kept. If information developed during a RFTF/VOTF investigation is included in such a form, the TFO's department will maintain the information as an agent of the RFTF/VOTF. No information related to RFTF/VOTF activities may be disseminated at any time to any third party (including a non-task

Page 2 of 3 Rev. 11/2020

force law enforcement officer, other law enforcement agency, or prosecutor's office) by any task force member without the express permission of the RFTF/VOTF Chief Inspector/Chief Deputy or his/her designee, in consultation with USMS Office of General Counsel where appropriate. This prohibition applies to formal and informal communications, as well as reports, memoranda, or other records compiled during the course of RFTF/VOTF operations. Documents containing information that identifies, or tends to identify, a USMS confidential source, a USMS sensitive program, or the use of sensitive equipment/techniques shall not be released outside of the USMS unless approved by the Office of General Counsel.

CONFIDENTIAL SOURCES / CONFIDENTIAL INFORMANTS: Pending the availability of funds, the USMS may provide funding for payment of Confidential Sources (CS) or Confidential Informants (CI). The use of CS/CIs, registration of CS/CIs and all payments to CS/CIs shall comply with USMS policy. USMS payment to an individual providing information or "tip" related to a USMS offered reward on an active fugitive case shall be accomplished by registering the individual or "tipster" through the established USMS CS payment process.

USE OF FORCE: All members of the RFTF/VOTF will comply with their agencies' guidelines concerning the use of firearms, deadly force, and less-than lethal devices, to include completing all necessary training and certification requirements. All members of the RFTF/VOTF will read and adhere to the DOJ Policy Statement on the Use of Less-Than-Lethal Devices, dated May 16, 2011, and their parent agencies will review the Policy Statement to assure that they approve. Copies of all applicable firearms, deadly force, and less-than-lethal policies shall be provided to the RFTF/VOTF Chief Inspector/Chief Deputy and each concerned TFO. In the event of a shooting involving task force personnel, the incident will be investigated by the appropriate agency(s). Additionally, in the event of a shooting, the required reporting for the FBI National Use of Force Data Collection (NUOFDC) should be accomplished by the involved task force personnel's employing agency when the TFO is inside their primary/physical jurisdiction and by the USMS when the TFO is outside their employing agency's primary/physical jurisdiction. If the employing agency wishes to submit such NUOFDC entries regardless of the physical location of the event, that is allowed under this MOU with prior written notice to the USMS.

NEWS MEDIA: Media inquiries will be referred to the RFTF/VOTF Chief Inspector/Chief Deputy. A press release may be issued and press conference held, upon agreement and through coordination with participant agencies' representatives. All press releases will exclusively make reference to the task force and participant agencies.

RELEASE OF LIABILITY: Each agency shall be responsible for the acts or omissions of its employees. Participating agencies or their employees shall not be considered as the agents of any other participating agency. Nothing herein waives, limits, or modifies any party's sovereign rights or immunities under applicable law.

EFFECTIVE DATE AND TERMINATION: This MOU is in effect once signed by a law enforcement participant agency. Participating agencies may withdraw their participation after providing 30 days advanced written notice to the RFTF/VOTF Chief Inspector/Chief Deputy.

Task Force:		
UNITED STATES MA	RSHAL or RFTF COMMANDER:	
Print Name:		
Signature:		Date:
PARTICIPANT AG	ENCY:	
Name: Cook County	Sheriff's Office	Phone: (312) 603-6444
Location (City and State	e): Chicago, Illinois / Cook County, Illinois	
PARTICIPANT AG	ENCY REPRESENTATIVE(S):	
Print Name and Title:	(b)(6); (b)(7)(C); (b)(7)(F) Deputy General Counsel	
Signature:	(b)(6); (b)(7)(C); (b)(7)(F)	Date: 8/27/2021
· ·		
INVESTIGATIVE O	OPERATIONS DIVISION:	
Print Name:		
Signature:		Date:

Page 3 of 3 Rev. 11/2020