United States Marshals Service

Privacy Impact Assessment
for the
Video Retention System

Issued by:

Charlotte Luckstone

Senior Associate General Counsel

Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [August 11, 2022

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

In 2020, the United States Marshals Service (USMS) procured and implemented a Video Retention System (VRS) to support the USMS implementation of the U.S. Department of Justice (DOJ) Body Worn Camera (BWC) Program for Task Force Officers (TFOs). The Attorney General (AG) executed an October 28, 2019, memorandum that authorized TFOs in certain cities to wear and utilize parent agency issued BWC on certain USMS-led Task Force operations. USMS ingests a copy of the footage as generated by the TFO into the VRS. Any copy of BWC footage obtained during a Task Force operation and shared with USMS is labeled a federal record and the original footage may not be released by a partner Agency without advanced written notification to the USMS.

On June 7, 2021, a DOJ memo via the Office of the Deputy Attorney General (ODAG) was disseminated to the heads of the USMS, Bureau of Alcohol, Tobacco, Firearms, & Explosives, Drug Enforcement Administration, and the Federal Bureau of Investigation (FBI) to develop a policy and a phased implementation plan for BWCs. As part of this expansion of BWCs to federal agents, the USMS commenced logistical planning and executed a procurement of its own BWC devices, as well as expanding the VRS to ingest BWC footage generated by Deputy United States Marshals (DUSMs). The USMS procured BWCs compliant with Federal Government mandates on Information Technology system's adherence to applicable laws, regulations, and rules. USMS use of BWCs is managed by the Body Worn Camera Program (BWCP).

The USMS VRS utilizes a vendor-purchased, Government-managed cloud service for content storage and management. DUSMs that are equipped with BWCs are required to attend an eight-hour training course developed by the USMS Training Division (TD), in collaboration with the BWCP, to be certified on the use of BWCs. The eight-hour training course includes instructions on program guidance, physical usage of the BWCs, the technical overview of the USMS' VRS platform, and other operational considerations. Furthermore, the program guidance instruction includes guidance on the protection of privacy and civil liberties.

After the adjudication of the Initial Privacy Assessment (IPA) and based on the collection of personally identifiable information (PII) by BWCs and the retention of said information in the VRS, it was determined that the USMS BWC technology required a Privacy Impact Assessment (PIA). As technology and operating environments change, this PIA will be updated and amended to reflect the analysis of how these changes affect the privacy interests of persons who directly or indirectly have contact with the information and data collection activities associated with USMS BWC operations.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The USMS VRS and BWCs will be primarily utilized by USMS for fugitive investigations (which includes fugitive escape cases), Emergency Support Function #13 (ESF-13) missions (i.e., where

USMS provides assistance to local, state, tribal, territorial, and Federal organizations after a natural/manmade disaster or an act of terrorism), missing child investigations, and USMS training purposes.

The USMS is authorized to investigate fugitive matters as directed by the United States AG. To achieve this mission, USMS executes arrest and/or search warrants at both first-party and third-party residences as part of Task Force operations that may include law enforcement from state and/or local agencies, as well as other federal agencies. In certain situations (e.g., where a third-party residence is involved and consent is not acquired), unless exigent circumstances exist, a search warrant may be obtained before entering the residence and/or any structure on the curtilage of the property. Upon sending a team of DUSMs and State or Local Partner Agency TFOs to a first-party or third-party residence, BWCs may be activated and BWC footage[1] may be captured.

With respect to the execution of a search and/or arrest warrant, the BWC is used to document the execution of said warrant and other spontaneous or adversarial contacts. The BWC footage is uploaded into the USMS VRS by the individual issued the BWC or their designee, following applicable chain of custody procedures. The footage is retained within the VRS as required by the Federal Records Act of 1950, 44 U.S.C. 3101. The VRS maintains the footage throughout the record lifecycle, ensuring appropriate access controls are applied and enabling authorized personnel access to video for authorized purposes. BWC footage may be reviewed by the DUSM taking that footage, their supervisor, the BWCP, or other entities on a case-by-case basis with authorization from the BWCP.

The BWC devices are USMS or Partner Agency issued devices only. No personally owned devices are allowed. While the TFO BWC devices may vary in make, model, or capabilities, the USMS BWC devices have a 12-hour battery life and can record up to 500-hours of footage with a storage capacity of 64-gigabytes. The USMS BWC devices store audio and video on encrypted internal memory and once physically connected to agency-issued single or multi-bay docking stations, the USMS BWC uploads recordings via an encrypted connection to the USMS VRS. No other destination for the BWC footage files is allowed nor available. The uploaded information is encrypted in transit and at rest within the USMS VRS.

For recordings related to TFOs, at the termination of an enforcement activity, the TFO will upload his or her BWC recording onto the TFO's parent agency's VRS. The TFO's parent agency has the original copy of footage captured on their agency-owned devices. The TFO's parent agency provides to the USMS a duplicate copy of the footage. The TFO's respective parent agency representative will create a partner agency share to the respective USMS Task Force Commander, USMS supervisor, or other authorized USMS personnel. The USMS personnel will validate the data provided and either accept or reject the data. Footage will be rejected if it does not apply to a task force operation.[2] If footage is rejected, the TFO will be informed that the footage was not accepted by the USMS. If accepted, the footage will go into the USMS VRS.

---

[1] As stated, the USMS body worn cameras, when activated, capture both video footage and audio content. Whenever this PIA references "footage," that reference also includes the corresponding audio recording.
[2] For example, if a TFO erroneously attempted to share footage relating to patrol work conducted while on a parent agency operation, such footage would be rejected by USMS.

For recordings related to DUSMs, the DUSM, or the designee, will upload his or her BWC recording into the VRS after the conclusion of an operation. The data will be managed as an official USMS record, also subject to all federal regulations, rules, policies, and procedures. DUSM BWCs only retain footage and metadata until the footage is uploaded in the VRS. Once ingested into the VRS, the BWC purges the footage, to include all associated metadata. The BWC has a battery life of approximately twelve hours. Additionally, the docking stations procured by USMS function in a pass-through capacity; they do not retain footage or have any storage capabilities. The docking stations simply allow footage to be transferred from the BWC to the VRS. Once the BWC footage is categorized at the time of ingestion, in connection with the DOJ policy on transitory records, the ingested BWC recordings will initially be reviewed and maintained during for a 180-day period. If the footage depicts an event of evidentiary value, USMS may retain the BWC recording for a longer duration and in accordance with USMS records retention schedules.

A BWC's internal memory (if the footage resides on the device prior to upload), as well as the VRS itself, collects, uses, processes, and stores "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked, or is linkable, to a specific individual," (i.e., PII). These recordings will contain the images of individuals and may contain address information (i.e., such as street name and number) as well as vehicle information, should any vehicle be in the driveway or on the curtilage of the subject residence. The BWC internal memory does not retain any PII other than that captured in the footage. Once uploaded into the VRS, the footage may also include additional metadata associated with the endeavor. In accordance with DOJ policy, the USMS will not retain for more than 180-days information collected using BWC that may contain PII, unless the retention of information is determined to be necessary for an authorized purpose or is maintained in a Privacy Act system of records.

Where retention of the data for longer than 180-days is necessary, the data collected will be retained pursuant to USMS Policy Directive 8.13 *Evidence,* and/or the relevant policies, procedures, and regulations governing such records retention (such as, the USMS records retention schedule for felony investigative files). BWC recordings will not be shared for any reason (i.e., to include law enforcement sharing requests) outside the USMS without permission first from the Office of General Counsel, the BWCP and (as appropriate), the Office of Public Affairs, the TD, and potentially the relevant U.S. Attorney's Office. Further, information sharing relating to the USMS BWCP 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.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	28 U.S.C. §§ 564 and 566(e)(1)(A), (B), and (D); 34 U.S.C. § 41503 ("Fugitive Apprehension Task Forces"); 18 U.S.C. § 2250 (Adam Walsh Child Protection and Safety Act of 2006).
	Executive Order	

X	Federal Regulation	Federal Rules of Criminal Procedure 41 – Search and Seizure
X	Agreement, memorandum of understanding, or other documented arrangement	Deputy Attorney General (DAG) Memorandum, *Body Worn Camera Policy* (June 7, 2021); AG's Memorandum Authorizing Body Worn Cameras by Federal Task Force Officers (October 28, 2019); Attorney General's Policy on Fugitive Apprehension in FBI and DEA Cases (August 11, 1988); AG's Memorandum, Implementation of National Anti-Violent Crime Initiative (March 1, 1994); U.S. Department of Justice Office of Legal Counsel Memorandum, Authority to Pursue Non-Federal Fugitives (February 21, 1995)
X	Other (summarize and provide copy of relevant portion)	USMS Interim Policy Directive 2.11 *Body Worn Camera (BWC)*

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	The names of targets of enforcement actions, third parties at the scene, and law enforcement officers present at the execution of the arrest and/or search warrant may be recorded by the BWC.
Date of birth or age	X	A, B, C, and D	Age of individuals may be discernable in BWC footage.
Place of birth			
Gender	X	A, B, C, and D	Gender of individuals may be discernable in BWC footage.
Race, ethnicity or citizenship	X	A, B, C, and D	Race and ethnicity of individuals may be discernable in BWC footage.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B, C and D	BWC footage could record the license plate numbers of cars located at a residence.
Personal mailing address	X	C and D	Home addresses may be captured in BWC footage.
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A and B	The serial number of the BWC completing the recording, and the USMS personnel who is associated with that particular camera are collected as part of the metadata associated with the BWC footage.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Law enforcement interviews of individuals conducted during the execution of a search and/or arrest warrant may involve questions pertaining to criminal history.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	GPS coordinates are collected by the BWC as metadata associated with footage. Additionally, location information may also be discernable in the BWC footage.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Captured data will include footage of arrestees, law enforcement personnel and potentially USPERs/Non-USPERs in the field of view of the capture device
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, and D	Captured data will include audio of arrestees, law enforcement personnel and potentially USPERs/Non-USPERs in the audio range of the capture device
- **Scars, marks, tattoos**	X	A, B, C, and D	Scars, marks, and tattoos of individuals may be discernable in BWC footage.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	A USMS e-mail address is used for account logon and access purposes.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Content of files accessed/reviewed**	X	A	As part of the information system's security, audit data will be automatically captured on content addition, access, modification and deletion.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Federal ID Number (FID) is used as an identifier for uploaded or shared content. Business information (such as, the physical address of a business) may be captured by the BWC. Additionally, because the BWCs capture audio and video recordings in a wide variety of settings, the types of PII captured will be extremely varied as well. The indications in this chart are only the PII that are considered likely to be captured, not all that may be or are possibly captured.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): Images and audio are collected by USMS or Partner Agency BWCs.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Agencies	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			

Government sources:
Other (specify):

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared as authorized and appropriate within USMS pursuant to DOJ (U.S. DOJ Policy on the Use of Body Worn Cameras, June 7, 2021) and USMS policies for law enforcement and/or training purposes compatible with the fugitive investigation, officer safety, ESF-13 mission, communication support, or missing child purposes for which the information was collected.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X			BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared through VRS as authorized and appropriate to other components of the DOJ pursuant to DOJ (U.S. Department of Justice Policy on the Use of Body Worn Cameras, June 7, 2021) and USMS policies for law enforcement and/or training purposes compatible with the fugitive investigation, officer safety, ESF-13 mission, communication support, or missing child purposes for which the information was collected.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X			BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared as authorized and appropriate to other federal entities pursuant to DOJ (U.S. Department of Justice Policy on the Use of Body Worn Cameras, June 7, 2021) and USMS policies for law enforcement and/or training purposes compatible with the fugitive investigation, officer safety, ESF-13 mission, communication support, or missing child purposes for which the information was collected. External sharing of BWC footage pertaining to an operational target will be governed by the provisions of the Warrant Information Network System of Records Notice and the routine uses of disclosure set forth therein.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
State, local, tribal gov't entities	X			BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared as authorized and appropriate to state entities pursuant to DOJ (U.S. Department of Justice Policy on the Use of Body Worn Cameras, June 7, 2021) and USMS policies for law enforcement and/or training purposes compatible with the fugitive investigation, officer safety, ESF-13 mission, communication support, or missing child purposes for which the information was collected. External sharing of BWC footage pertaining to an operational target will be governed by the provisions of the Warrant Information Network System of Records Notice and the routine uses of disclosure set forth therein.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Public	X			BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared as authorized and appropriate with the public in response to Freedom of Information Act (FOIA) requests or other public records requests. External sharing of BWC footage pertaining to an operational target will be governed by the provisions of the Warrant Information Network System of Records Notice and the routine uses of disclosure set forth therein.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			BWC recordings, maintained in the VRS and retained in accordance with the USMS DOJ evidentiary or other policies or procedures (e.g., USMS Interim Policy Directive 2.11 *Body Worn Camera*) may be shared as authorized and appropriate with prosecutorial or other legal entities (e.g. defense counsel) for law enforcement and/or litigation purposes. External sharing of BWC footage pertaining to an operational target will be governed by the provisions of the Warrant Information Network System of Records Notice and the routine uses of disclosure set forth therein. Additionally, the sharing of records in connection with litigation where the United States is not a party will be governed by the USDOJ *Touhy* regulations, located at 28 C.F.R. 16.21 et seq.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Not applicable.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of

Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Generally, no notice will be provided to individuals whose PII may be captured by the BWC during a USMS enforcement operation(s) and/or other activities that is permitted under USMS Interim Policy Directive 2.11 *Body Worn Camera,* that is retained on the BWC or VRS. Providing notice to those individuals who are subjects of USMS operations (such as, subjects of the execution of an arrest and/or search warrant where a BWCs will be activated) would effectively inform those individuals of planned USMS enforcement operations and give fugitives or persons of interest the opportunity to take action to undermine USMS operations. Informing fugitives of planned USMS operations would minimize the effectiveness of those operations and increase the risk on public safety as advanced knowledge of arrest and search operations would increase the flight of individuals wanted by law enforcement. However, there are certain state jurisdictions where consent of all parties to a recording of an oral communication is required, otherwise known as a "two-party" ,"all-party" notice, or consent states where law enforcement is not excepted. In such jurisdictions, when engaged in enforcement actions related to adopted state/local arrest warrants (or associated search warrants) for which BWC recordings are required or permitted under the DOJ and USMS Interim Policy Directive 2.11 *Body Worn Camera* and procedures, the USMS will inform individuals that they are being or have been recorded as soon as practicable and when it is safe to do so.

Once the BWC recording is uploaded into the VRS, the information becomes a part of the USMS investigatory file on a target. Dissemination of USMS evidentiary records retained in a federal system of records is done in connection with the protections and provisions located in the Privacy Act. USMS files pertaining to the target of a federal or state arrest warrant are subject to the provisions in the Warrant Information Network (WIN) SORN, located at https://www.govinfo.gov/content/pkg/FR-2007-03-05/pdf/E7-3757.pdf. This PIA, once completed and published, will also serve as a generalized notice to the public on BWC usage by the USMS.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals do not have the opportunity to consent to the collection, use, or dissemination of information collected by the BWC because the individuals' images or information is collected subject to USMS enforcement operations (e.g., subjects of the execution of an arrest or search warrant). Allowing individuals an opportunity to consent in this context would minimize the effectiveness of those operations and increase the risk on public safety, as advanced knowledge of arrest and search operations would increase the flight of individuals wanted by law enforcement.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Members of the public may file Privacy Act or Freedom of Information Act (FOIA) requests, as

appropriate, for BWC recordings. Information regarding how to file a FOIA/PA request with USMS can be found at: https://www.usmarshals.gov/freedom-of-information-act. Records can be processed and released to the requestor subject to appropriate withholdings. Records of individuals not relevant to the request will be appropriately redacted prior to release. Similarly, federal or state defendants whose image was captured may pursue release of the BWC recording for use in litigation via the DOJ *Touhy* Regulations, 28 U.S.C. § 16.21, et seq., or other federal discovery procedures.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): The ATO is current and set to expire on February 17, 2024 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** The VRS, is a Cloud-based commercial system, purchased from Axon Incorporated, but operated and maintained by USMS full time employees and/or designated contractors. The VRS operates in Axon's Federal Government Cloud instance and is governed by the General Services Administration (GSA) FedRAMP ATO process. The VRS is considered a major system within the USMS and therefore sought and received its own Authorization to Operate. BWCs and the VRS were tested for compliance with security controls during the acquisition process and subsequent Pilot phases. USMS employees who are designated by their supervisors to perform roles within USMS-Net and have been issued proper security badges and passwords, will have access to this system and the minimum information necessary to perform their job duties. USMS employees receive training on the proper safeguarding of personally identifiable information. The system tracks access logs and maintains an electronic audit trail to protect against unauthorized access. USMS employees with access to VRS treat PII in accordance with a National Archives and Records Administration-approved record retention schedules and in a manner that prevents loss, theft, misuse, or unauthorized access. Security measures for VRS have been implemented in accordance with federal guidelines categories of: Access Control; Awareness and Training; Audit and Accountability; Certification, Accreditation, and Security Assessments; Configuration Management; Contingency Planning; Identification and Authentication; Incident Response; Maintenance;
X	Media Protection; Physical and Environmental Protection; Planning; Personnel Security;

	Risk Assessment; System and Services Acquisition; System and Communications Protection; and System and Information Integrity.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** USMS use of BWC footage is in the initial phases, where the upload, storage, and maintenance of recordings from BWCs are being constantly evaluated. BWC recordings are being monitored by both the USMS BWCP personnel but also the USMS Information Technology Division (ITD). The BWCP monitors the safeguarding of data confidentiality, and that data is only used for authorized purposes and the ITD monitors and evaluates data availability, confidentiality, and integrity as per USMS, DOJ and US Government requirements.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The VRS has a robust auditing capability as well as access controls to protect against unauthorized use and access. USMS employees who are designated by their supervisors to wear BWCs or perform roles within VRS are issued proper security badges and passwords. Only these specific employees will have access to the VRS system and the minimum information necessary to perform their job duties. All USMS employees, including those with access to VRS, receive yearly training on the proper safeguarding of personally identifiable information through the Computer Security Awareness Training. The VRS tracks access logs and maintains an electronic audit trail to protect against unauthorized access and dissemination of the information therein. When the BWC uploads a recording to the VRS, and the data on the VRS is retained, the data becomes subject to USMS Policy 8.13, *Evidence*. USMS Policy 8.13 states that all evidentiary items will be seized according to statutory authority, preserved until collected by appropriate personnel, transferred pursuant to chain of custody procedures when applicable, and stored until final disposition.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Contractors are not permitted to use BWCs as part of enforcement actions, but may have access (as a result of job-specific duties) to the footage file that contains PII collected by BWCs once uploaded to the VRS. Any contractors involved in the BWC program work under the oversight of USMS Federal Employees.

X	**Each component is required to implement foundational privacy-related training and a refresher privacy training annually for all component personnel which includes employees, interns, and contractors when they onboard. . Indicate whether there is additional training specific to this system, and if so, please describe:** DUSMs are required to attend the USMS BWC Training Course prior to USMS approval to wear BWCs. This training includes instruction on relevant USMS and DOJ policies, appropriate case law, the Constitution, as well as device operating parameters. Supervisors who are authorized to review their employees' BWC footage(s) are also required to be trained on the same policies, procedures, and protection of privacy and civil liberties. Further, Supervisors, Task Force Commanders, and Team Leads assigned to enforcement operations require training specific to the TFO BWC guidelines.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

BWCs will be primarily utilized by USMS for enforcement operations and fugitive investigations, which includes fugitive escape cases, where the BWC is used to record DUSMs and/or TFOs on approach to the residence, monitor the entrance to the residence and any exits of the residence, and view any structures on the curtilage of the property. BWCs will also be utilized for ESF-13 missions (i.e., where USMS aids local, state, tribal, territorial, and Federal organizations after a natural/manmade disaster or an act of terrorism), radio communications support, missing child investigations, USMS training purposes, and other missions as assigned by the USMS Director. Once an operation has ceased, BWCs will be deactivated, and video/audio recording will cease. If BWCs are deactivated due to a scene being declared secure and an exigent situation arises, DUSMs will reactivate their BWCs as soon as safe and practical to do so. Footage from BWCs are uploaded to the VRS, corresponding with the name of the DUSM or TFO that made the recording, the date and time of the recording, and in certain instances with compatible cameras, the serial number of the camera having made the recording.

USMS employees who are designated by their supervisors to perform roles within VRS and have been issued proper security badges and passwords, will have access to this system and the minimum information necessary to perform their job duties. USMS employees receive training on the proper safeguarding of personally identifiable information. The system tracks access logs and maintains an electronic audit trail to protect against unauthorized access.

Where retention of the collected footage beyond the 180-day transient record period on the VRS is necessary, the data collected will be retained pursuant to USMS Policy Directive 8.13, *Evidence*, and/or the relevant policies, procedures, and regulations governing such records retention. Footage will be marked with an appropriate retention category to ensure appropriate records disposition and retention. BWC recordings retained on the VRS will not be shared for any reason (to include law enforcement sharing requests) outside the USMS without permission first from the OGC, the BWCP and (as appropriate), the Office of Public Affairs, the TD, and potentially the relevant U.S. Attorney's Office.

The service is hosted on a GSA FedRamp-High certified Microsoft Azure cloud environment. USMS' instance of VRS is segregated from other instances logically by utilizing access controls such as Active Directory Single Sign-On tied to a USMS employee's DOJ Justice Consolidated Network (JCON) account, access control lists (ACLs), VRS roles, permissions granted by authorized USMS personnel and by approved network Internet Protocol (IP) addresses. ACLs and IP address restrictions are set and managed by USMS personnel and tracked by the USMS ITD IT Change Management process.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

In accordance with DOJ policy, the USMS will not retain information collected using BWCs that may contain PII for more than 180-days, unless the retention of information is determined to be necessary for an authorized purpose or is maintained in a Privacy Act system of records. Authorized purposes may include, but are not limited to, law enforcement investigations, litigation, and training. Absent such an authorized purpose or maintenance in a Privacy Act system of records, it is USMS policy to purge all recordings obtained by the BWCs and uploaded into the VRS upon completion of the 180-day transient record retention guidelines, unless some other critical or reportable incident occurs. In these circumstances, the recording will be held in accordance with USMS guidelines for records retention. BWC footage is classified under the appropriate records retention schedule depending on why the footage is retained. As it pertains to an individual arrested for a felony, the footage is retained pursuant to the Felony Investigative Files records schedule (as the footage is another piece of evidence associated with the case). Footage retained as responsive to other types of requests (such as footage relevant to civil litigations, tort claims, FOIA requests, etc.) is retained in accordance with the appropriate USMS or DOJ schedule for said records.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

USMS files pertaining to the target of a federal or state arrest warrant are subject to the Warrant Information Network System of Records Notice (SORN), located at: https://www.govinfo.gov/content/pkg/FR-2007-03-05/pdf/E7-3757.pdf.

The Warrant Information Network SORN covers individuals for whom a federal, state, or local warrant was issued, when the warrant is part of a USMS sponsored multi-agency Task Force;

individuals suspected in a state case that has been adopted by a USMS sponsored Task Force; individuals for whom the USMS is conducting a criminal investigation or aiding in a criminal investigation by another law enforcement agency; missing persons, including children, for whom the USMS is conducting an investigation or aiding in a criminal investigation by another law enforcement agency; and, individuals and their associates, who are the subject of, and who may provide information, assistance or leads in USMS fugitive, criminal, or missing persons investigations. This SORN covers both computerized records pertaining to the execution of arrest and search warrants, as well as the complete investigatory file pertaining to a target.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

During the initial setup of the VRS, prior to the DOJ mandate for Federal Law Enforcement Officers to wear BWCs, the USMS recognized the risk to privacy should unauthorized access to TFO BWC footage occur. The USMS Investigative Operations Division and ITD undertook a rigorous evaluation and configuration effort to ensure that only authorized personnel have access to authorized data for authorized purposes. Program governance and processes were developed and tested prior to fielding the system. The program governance and processes defined that access to the system is granted through the USMS Account Management process and access follows the least privilege model to ensure only access is only granted to the least amount of data required to successfully achieve the USMS mission for any given individual. Individuals with authorized access to the initial instance of the VRS were required to be USMS employees or contractors that had successfully completed all badging and credentialling processes, along with the Computer Security Awareness Training (CSAT) as mandated by the agency on an annual basis.

When the USMS was mandated to obtain and field its own BWCs for use by DUSMs, the agency re-used and enhanced the existing data protections such as access control groups, integration with agency authentication services, and enhanced auditing features. The model for DUSM BWC integration also includes the least privilege access model, limiting access to DUSM BWC footage to the operational individual with the BWC[3], their supervisor[4] and the BWCP. Other access is granted for authorized purposes on a case-by-case basis[5]. TFOs are required to attend a two-hour training session prior to

[3] Per USMS policy, a DUSM may review their own BWC recording. Their review is captured by the VRS audit log.
[4] Per USMS policy, a DUSM's supervisor may review a DUSM's BWC recording only for authorized purposes. Those purposes include but are not limited to: review of critical incidents, training concerns or random audits for program compliance. These reviews are also captured in the VRS audit log.
[5] USMS is cognizant of the privacy-related risks inherent in allowing a DUSM, their supervisor or other individuals the ability to review footage. There exists the possibility of an agency issued phone or personal phone could capture a recording, and/or a DUSM viewing the recording could screenshot the recording and disseminate that screenshot, and/or a DUSM could allow for unauthorized access to the website by disseminating his or her login information. However, USMS also notes that all USMS employees, to include TFOs affiliated with state or local agencies, are subject to rigorous background investigations. DUSMs and TFOs are required to consent to the USMS Code of Professional Conduct and Rules of Professional Responsibility prior to employment and involvement on a USMS led task force operation. DUSMs, TFOs, and contractors are instructed not to disseminate login information to the website where BWC recordings can be

any operational deployment of BWCs. In the future, a refresher training on LearnUSMS (developed by the TFO Program Coordinator in conjunction with the USMS Office of the General Counsel (OGC)) will be required. Prior to being authorized to wear a BWC, in addition to the badging/credentialling and CSAT course that USMS employees or contractors must complete, a DUSM or Supervisor must also complete an eight-hour training course provided by the USMS TD in collaboration with the BWCP. The eight-hour training course includes instructions on program guidance, physical usage of the BWCs, technical overview of USMS' VRS, and other operational considerations.

In accordance with DOJ policy, the USMS will not retain information collected using BWCs that may contain PII for more than 180-days, unless the retention of information is determined to be necessary for an authorized purpose or is maintained in a Privacy Act system of records. In these circumstances, the recording will be held in accordance with relevant the USMS guidelines for records retention.

Once the BWC recording is uploaded into the VRS, the file becomes a part of the USMS investigatory file on a target. Dissemination of USMS evidentiary records retained in a federal system of records is done in connection with the protections and provisions located in the Privacy Act. As previously indicated, USMS files pertaining to the target of a federal or state arrest warrant are subject to the WIN SORN, located at https://www.govinfo.gov/content/pkg/FR-2007-03-05/pdf/E7-3757.pdf. This SORN covers both computerized records pertaining to the execution of arrest and search warrants, as well as the complete investigatory file pertaining to a target. The WIN SORN sets forth limited routine uses, whereby agency records may be shared for specified purposes without the consent of the individual to whom the record pertains. Further, information sharing relating to BWCP footage 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.

The USMS has utilized the embedded VRS features such as role-based access and access control lists to control unauthorized access to data. Based on the way the VRS has been designed, alteration of a original source footage is not possible. Some data elements of the metadata pertaining to a piece of footage may be updated or modified, but never the source footage. Any data modification is captured by a robust auditing capability that cannot be altered by a USMS user and available for review by authorized USMS personnel.

As for risk mitigation with the BWC devices themselves, the BWC is assigned to the USMS VRS at installation time. Once assigned, the BWC cannot be assigned or utilized with another VRS account without first needing to be wiped of the original assignment data, which can only be completed by authorized USMS personnel. If a device is lost or stolen, a device's data will be inaccessible due to being encrypted. Additionally, it is protected by USMS user credentials, and inaccessible by anyone not in the USMS VRS and assigned the individual camera (meaning, a member of the public cannot access the footage on the VRS). With the integration of cellular and GPS in the device, if a BWC is

---

viewed and instructed against disseminating any portion of the recording. Each DUSM, TFO, and contractor is given yearly training by USMS on safeguarding law enforcement sensitive information. Any violation of the Rules of Professional Behavior, Code of Professional Conduct, and/or USMS policies on safeguarding law enforcement sensitive information will be forwarded to and handled by the appropriate disciplinary officials as soon as practicable.

marked lost or stolen and is powered on, the USMS VRS will alert system administrators as to the whereabouts of the device. In addition to the software protections, other than the USB-C charging port, the BWC device is a physically closed system. All system components are direct soldered together, with no user removable or serviceable parts.