Drug Enforcement Administration

Privacy Impact Assessment
for the
DEA Body-Worn Camera Program

Issued by:
David J. Mudd
DEA Senior Component Official for Privacy

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

Date approved: August 17, 2022

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

This privacy impact assessment (PIA) analyzes the Drug Enforcement Administration's (DEA) body-worn camera (BWC) program, specifically the two interconnected technology solutions that comprise the BWC program: the cameras and the associated information system. The cameras that will be worn and used by DEA agents are Axon cameras, and the associated information system is the FedRAMP authorized Software as a Service (SaaS) Axon cloud platform Evidence.com (Ecom). Axon cameras allow video to be directly uploaded to Ecom via a docking station where the video footage can be accessed in accordance with controls discussed in more detail throughout the PIA. Other cameras may be used by DEA-deputized task force officers (TFOs), if required by the TFO parent agency. In that case, Ecom is able to receive the video from non-Axon cameras via a separate process, also detailed below. The BWC program will be owned and managed by DEA's Office of Operations Management (OM).

As background, on October 28, 2020, the Department of Justice (DOJ) announced a policy that permits state and local officers serving on DOJ Task Forces (known as TFOs) to wear and activate body-worn cameras (BWCs) when the use of force is possible – while serving arrest warrants, executing other planned arrest operations, and during the execution of search warrants. *See* Interim Standard Operating Procedures for Task Force Officer Body-Worn Camera Program.

On June 7, 2021, Deputy Attorney General (DAG) Lisa Monaco directed the Department's law enforcement components, including the DEA, to issue BWC policies that require agents to wear and activate BWC recording equipment for purposes of recording their actions during: (1) a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, including the apprehension of fugitives sought on state and local warrants; or (2) the execution of a search or seizure warrant or order. Further, the DAG directed that "[e]ach law enforcement component shall develop its policy and a phased implementation plan for compliance with the above directive[,] … including procedures governing the use of BWCs by all members of Department-sponsored task forces." *See* Memorandum from Deputy Attorney General Lisa Monaco, *Body-Worn Camera Policy*. DEA has issued an interim BWC policy and an implementation process and will be using the Axon technologies discussed in this PIA in accordance with those policies and procedures.

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 purpose of the DEA BWC program is to foster public trust by increasing transparency and accountability of law enforcement operations, while also modernizing our access to video evidence and operational reporting and creating a more thorough and accurate evidence record. To that end, DEA agents and TFOs will wear and activate Axon cameras for purposes of recording their actions during: (1) a pre-planned attempts to serve an arrest warrant or other pre-planned arrests, including the apprehension of fugitives sought on state and local warrants; or (2) the execution of a search or seizure warrant or order.

Axon cameras are clearly visible and are mounted on the outside of an officer's uniform. They collect video in 1080p resolution and MPEG-4 format, have a battery life of 12 hours of recording operation and contain 64 gigabytes of storage. Each camera has a unique number that is assigned to an individual agent and is reflected in the Ecom system as well. The cameras can be turned on and off manually, and they can be set up to turn on automatically when an officer draws a weapon or activates emergency lighting. DEA is not planning on using the automatic on/off function at this time. The cameras have the capability to live stream video via an internal cellular modem to an Axon command application where authorized recipients can view the live footage. DEA is not planning to use the live streaming capability at this time. The cameras do not have facial recognition capabilities or any other biometric collection or analysis capabilities.

The Axon View is a mobile application that allows the user of an Axon BWC to view the video currently on the camera prior to uploading it to the Axon digital evidence management system. The application is password protected and is paired directly with the agent's camera. The agent is unable to make any changes to the video at any time.

Video from Axon cameras is then uploaded into the Axon cloud platform Evidence.com, which allows officers and their designated, pre-authorized supervisors to view the video footage and create a written transcript of audio collected from the video. For DEA BWCs, the video transfer must be done "physically" by placing the BWC in a docking station, which has a hard wire connection to the internet. To upload the camera footage, Ecom requires a "handshake" double key authentication with the server, which is done by docking the camera via physical connection with an Axon dock that has a proper mobile or hard-wired internet connection, or via USB to a DEA workstation or laptop (connected by hardwire to the internet) and utilizing the Axon View XL application to complete the upload. The transfer can also take place on a stand-alone laptop or desktop computer, but the preferred method is via docking station or USB to a DEA workstation or laptop. Once this is done, the video starts to transfer, sending smallest files first and working is way to larger videos. Once a video is sent, the server receives the packets, verifies them, then confirms its completion or failure with the camera. On a verified completion, the camera then deletes the video off of the device. On a failed transfer, the camera will restart the transfer from the beginning. This will happen for every video on the camera until all video is offloaded. If the camera is removed from the dock during transmission, this approach prevents video loss. The data is encrypted on the cameras locally and in transit.

For non-Axon cameras used by TFOs, any DEA Ecom user or an Ecom administrator can send a TFO a link for a one-time upload, and the TFO could upload when logged in the TFO's Ecom account. The TFO would be able to send a link to any non-Axon account in the same manner for a one-time upload. TFOs also have the option of logging on to their Ecom account and uploading video using the evidence portal. The non-Axon camera never gets connected to the Ecom account. Rather, the TFO's non-Axon camera video would be uploaded to the non-Axon cloud. The video from the non-Axon cloud to the DEA Ecom account would be uploaded into Ecom through end-to-end encryption. It does not use

iPhone technology nor is there a hardwired physical connection between the non-Axon camera and Ecom.

Agents, TFOs, and supervisors log into Ecom from any mobile or hard-wired internet connection via two-way authentication, with a username and password and a verification code sent via text or email. Inside the system, individuals can only view their own videos and videos of any subordinates assigned to them in the system. Ecom accomplishes this by group permissions and has monitoring and auditing controls to view all user activities in the system (see section 6 for further detail). The audit log created by Ecom would detect inappropriate copying or sharing of the video, which would result in follow up and potential consequences for the user. Any action involving the video (upload, viewing, exporting, etc.) is logged by Ecom in the audit trail. Video can also be shared with other components that are using Ecom, though DEA is not currently using this feature and is in the process of determining what level of permission or authorization is required before video can be shared. Video copies can also be made and exported, and personnel must comply with all DEA BWC policies related to copying and handling evidence. Videos have different retention schedules and can be assigned viewing restrictions based on the type of operation in which they were created. After the retention period has expired, videos go into a 30-day holding period and are not eligible for deletion until that period has expired.

DEA policy requires that Special Agents be trained in the operation of BWCs, DEA's BWC Policy, and legal issues associated with BWC use, prior to operational use of BWCs. As part of DEA's phased implementation plan, DEA will provide this training when the Special Agents are issued BWCs and prior to operational use. DEA's goal is to have all Special Agents trained and operational within five years. In those locations, TFOs are also required by DEA policy to receive DEA BWC training (including TFO non-Axon cameras for DEA task force use) or Ecom. Currently, this DEA BWC training is provided by DEA's Office of Chief Counsel, Office of Compliance, and Axon but will eventual be delegated to the Field divisions.

As a part of DAG Monaco's Body-Worn Camera Policy, each DOJ component, including DEA, is required to submit a PIA to the Office of Privacy and Civil Liberties prior to implementation of its BWC policy, and is also required to provide OPCL as soon as practicable with a plan for an annual privacy review of the BWC program. This PIA submission to OPCL accomplishes both tasks. DEA's plan for annual privacy reviews of its BWC program is as follows:

DEA will continuously monitor the BWC program for significant changes, first through the DEA's Senior Component Official for Privacy (SCOP's) presence on the Information Technology Acquisition Review Board, which must review and approve any financially significant technology purchase. Second, DEA's Chief Counsel will be closely involved with the daily operations of the program during the five year roll out due to Chief Counsel's role in training agents. Finally, the DEA SCOP will make a formal inquiry to the lead program office, OM or otherwise, every year following the finalization of this PIA as to any possible significant changes to the program that may not have been noted using the first two methods. This inquiry will coincide closely in time with the annual Federal Information Security Modernization Act (FISMA) report so the SCOP will make the annual inquiry at that time each year. Areas of inquiry will include, but not be limited to:

- A description of changes over the past year, or foreseen for the next year in how the DEA:
    - Collects BWC data
    - Stores BWC data
    - Shares/grant access to BWC data
    - Searches through BWC data
    - Protects all BWC data, or particularly sensitive BWC data
- Any breaches involving BWC data. (Number and type of such breaches.)

- Lessons learned generally from that year's use.
- Any feedback from DEA agents/TFOs on difficulties or success stories and how that might impact privacy/civil liberties aspects (for example, what or how info is collected, how or how long it is stored or shared).
- Number of FOIA or Privacy Act requests involving BWC data, and outcomes.
- Cloud service provider issues that may impact privacy. (Changes in provider, or contract language, or access protocols, or audit log capabilities.)

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	The Controlled Substances Act, 21 U.S.C. Section 801 *et seq.*
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	Memorandum from Deputy Attorney General Lisa Monaco, *Body-Worn Camera Policy*, June 7, 2021. Department of Justice Policy on Use of Body Worn Cameras by Federally Deputized Task Force Officers, October 29, 2020. DEA Interim Policy for DEA Body-Worn Camera Program

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 D	Names of arrestees or owners or tenants of premises searched likely to be collected and audio could potentially capture such information incidentally for anyone named, including employees and task force officers.
Date of birth or age	X	A B C D	Inferred from video or audio.
Place of birth			
Gender	X	A B C D	Inferred from video.
Race, ethnicity or citizenship	X	A B C D	Inferred from video.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license	X	C D	Driver's license image could be recorded or number mentioned incidentally.
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A B C D	Inferred from video or audio.
Personal mailing address	X	C D	Addresses could be recorded or mentioned incidentally.
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	X	A B C D	Uniforms can be captured on video, indicating military status, rank, awards, etc. or audio could capture military information discussed
Employment status, history, or similar information	X	A B C D	Video could capture information related to employment.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A B C D	The presence of mobile devices will be captured on video, but the cameras do not analyze mobile devices.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A B C D	Arrests will be recorded. Video or audio could potentially capture additional information incidentally.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A B C D	Video could record civil law violations or audio could record allegations.
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A B C D	Video or audio could be used to identify potential witnesses or record other witness 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 D	Video or audio could be used to identify locations.
Biometric data:			
- **Photographs or photographic identifiers**	X	A B C D	Any still images from video will not contain any special biometric isolation or analysis capabilities.
- **Video containing biometric data**	X	A B C D	The videos will not contain any special biometric isolation or analysis capabilities.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A B C D	Voices will be recorded, but the BWC program will not create voice profiles or track individuals using a voice pattern.
- **Scars, marks, tattoos**	X	A B C D	Video could capture images of scars, marks, or tattoos.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A B	
- **User passwords/codes**	X	A B	
- **IP address**			
- **Date/time of access**	X	A B	
- **Queries run**	X	A B	
- **Content of files accessed/reviewed**	X	A B	
- **Contents of files**	X	A B	

(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
Other (please list the type of info and describe as completely as possible):	X	A B C D	*Because the cameras will collect video and audio at unpredictable and varied times and locations, it is possible that any data element listed here, as well as others, could be recorded. However, DEA is only marking the chart for data types that will be collected regularly and as a part of the BWC program's intended purpose.

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):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
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	DEA agents and TFO's can view their own videos and their supervisors can view videos of personnel within their authorized group. Copies can also be made and shared within DEA, subject to BWC policy limitations, including a legitimate need to know.
DOJ Components	X			If other DOJ components use Ecom, DEA users will eventually be able to search for those outside users and share video files with them, after receiving permission from an appropriate-level supervisor, to be determined by DEA. Videos can also be copied and shared, subject to policy limitations.
Federal entities	X			In accordance with policy and applicable routine uses. Access is case-by-case.
State, local, tribal gov't entities	X			In accordance with policy and applicable routine uses. Access is case-by-case.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			BWC videos are made available through the discovery process. Copies can be made of videos, which can be shared and used for purposes of criminal prosecution.
Private sector				
Foreign governments				

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.**
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.

DEA does not intend to share BWC program data for Open Data purposes or for research or statistical analysis.

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.

Agents and TFOs will receive training on the Axon technologies and will be required to comply with DEA's BWC policy, so they will be aware of how any recorded information about them can be accessed, shared, and used. In addition, regarding recorded information about persons who are not agents or TFOs doing the recording, to the extent that BWC data becomes Privacy Act records in a system of records, notice would be provided in the applicable system of records notice published in the Federal Register, DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21,808 (April 11, 2012) (last published in full).

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.

Since information is collected in connection with criminal justice interactions and investigations, individuals generally do not have the opportunity to object to the collection of this information. Agents and TFO's will be able to participate voluntarily in the collection, use, and dissemination of their own videos through the Ecom platform as described above, though the use of the cameras in pre-established circumstances is mandatory, and it is possible that certain video sharing activities will also be required by law or policy, such as sharing with parties pursuant to a court order. So there will be voluntary and involuntary aspects to collection, use, and dissemination on the part of agents and TFOs.

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.

Individuals are free to exercise their rights to access and amendment under the FOIA or the Privacy Act, however information may be redacted under the FOIA, and DEA-008 is subject to certain exemptions to the access and amendment provisions of the Privacy Act, as described and authorized in 28 C.F.R. Section 16.98.

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).

X	**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 was authorized May 20, 2022 **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:**
	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:** For both the Axon cameras and Ecom, monitoring, testing, and evaluation are conducted as required by NIST, FedRAMP, and part of the ATT and ongoing ATO process.
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:** For the system as a whole, which is comprised of the Axon cameras and Ecom, the ATO will be renewed at least every three years, unless the system is part of the Ongoing Authorization Program. The system will undergo a thorough security review as required by the relevant authorization process. The program will also be reviewed on an annual basis for significant new risks to privacy, which would require a new or amended PIA. Within the system, Axon creates an audit log for all access to each account and all video viewing within that account. These auditing trails can be reviewed at any time by authorized DEA supervisors with the necessary permissions. DEA will work with Axon to ensure that their administrator access aligns with DEA requirements.
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**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Training specific to

	the Axon cameras and cloud is provided to each field division when they receive the technology and to each agent who will use them. This training is provided by Axon, DEA Chief Counsel, and DEA Office of Compliance.

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?

Working through the technology's data flow, the first privacy concern is over collection by the agents and TFOs in the field. This is mitigated by a strict policy on what activities can and must be recorded (including audio and video), which users must read and adhere to. Cameras are to be used only during: (1) a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, including the apprehension of fugitives sought on state and local warrants; or (2) the execution of a search or seizure warrant or order. In addition, specific training is provided by multiple stakeholders on how to operate the equipment properly and how to comply with DOJ and DEA policies. DEA has made the decision not to utilize the system's automatic on/off switch or its live streaming feature at this time.

Next, security is protected during transfer to the Axon cloud, Ecom. Data is encrypted at rest and in transit. Ecom requires a "handshake" double key authentication with the server, which is done by docking the camera with an Axon dock that has proper internet connection. Once this is done, the video starts to transfer, sending smallest files first and working is way to larger videos. Once a video is sent, the server receives the packets, verifies them, then confirms its completion or failure with the camera. On a verified completion, the camera then deletes the video off of the device. On a failed transfer, the camera will restart the transfer from the beginning.

Ecom requires two-factor authentication to access the system. Inside the system, users can only access their own videos, via their account, as well as any subordinate's videos, established by group permissions. Every account log in and video viewing is logged. Videos are tagged and categorized according to context and sensitivity, for instance all videos of service of arrest warrants will be labeled as such, and videos that involve the use of force will be labeled as such, in addition. If an agent has to view a sensitive video multiple times, he or she is able to leave comments about why an abnormal level of attention is necessary. Authorized DEA personnel with appropriate system permissions can limit the number of views possible for sensitive videos, and any sharing of videos with other Ecom users must be authorized by an appropriate DEA personnel. The DEA personnel who have control over the number of times a video can be viewed and who can authorize sharing is limited to: 1) the "owner" of the video, which will typically be the SA or TFO who recorded and uploaded the video; and 2) supervisors in the "owner's" chain of command. (GS/ASAC). The Point of Contact/System Administrator for each division will also have the aforementioned permissions.

Regarding the sharing of video outside of DEA in Evidence.com, the same DEA personnel listed above can authorize the sharing. The sharing can be limited to a specific timeframe and the "sharer" can limit the amount of times the video is viewed or downloaded. The "sharer" can also share the video in a manner that the "sharer" can designated it as "view only" or "download only."

Regarding how the video sharing is documented, the audit trail created by Ecom for the specific video will show who shared the video, when it was shared, who viewed or downloaded the video and when the viewing or download took place. In addition, Axon personnel are not able to access any DEA videos

stored in Ecom. There are no "backdoors" or "peering points" by which Axon personnel could access the videos. The instance is created by granting a DEA user a "super user" permission set, as opposed to Axon personnel, beginning with account access and passing those permissions on to others in DEA at a later date. This system is an implementation of the FedRAMP authorized, Axon - US Axon FedCloud solution. As such, the cloud service provider's compliance with monitoring privileged user activity is monitored by FedRAMP and the Third-Party Assessment Organization (3PAO). The DEA, specifically the System Owner in consultation with the Information System Security Officer, reviews the CSP provided audit logs for indications of inappropriate or unusual activity for both privileged and general DEA users of the system.

This video categorization capability will also allow for DEA to tailor disposal procedures. Each type of evidence will be maintained in accordance with its related records schedule, and there is an additional 30-day period after the expiration of the retention schedule where videos are moved to a cache and cannot be completely deleted.

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.)

Retention for arrest/arrest warrant, search/seizure order, and all other enforcement activities is 25 years. Retention for training videos is 30 days. Once the retention period has expired, videos are moved into a pre-deletion cache for an additional 30 days and are deleted thereafter.

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.

BWC data does not constitute Privacy Act records in a system of records as the data is maintained in Ecom because videos are not retrieved by personal identifier. However, if the data is copied and moved into an investigative case file as non-drug evidence, it will be covered by DEA-008.

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:

DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21,808 (April 11, 2012) (last published in full).

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?

a. ***Potential Threats Related to Information Collection***

Working through the technology's data flow, the first privacy concern is over collection by the agents and TFOs in the field. This is mitigated by a strict policy on what activities can and must be recorded, which users must read and adhere to. Cameras are to be used only during: (1) a pre-planned attempts to serve an arrest warrant or other pre-planned arrest, including the apprehension of fugitives sought on state and local warrants; or (2) the execution of a search or seizure warrant or order. In addition, specific training is provided by multiple stakeholders on how to comply with these policies, and DEA has made the decision not to utilize the system's automatic on/off switch or its live streaming feature.

b. Potential Threats Related to Use and Maintenance of the Information

Next, security is protected during transfer to the Axon cloud, Ecom. Data is encrypted at rest and in transfer. The Axon cloud has achieved FedRAMP Joint Authorization Board Provisional Authority to Operate (P-ATO) at the moderate impact level. Ecom requires a "handshake" double key authentication with the server, which is done by docking the camera via physical connection with an Axon dock that has proper mobile or hard-wired internet connection. Once this is done, the video starts to transfer, sending smallest files first and working is way to larger videos. Once a video is sent, the server receives the packets, verifies them, then confirms its completion or failure with the camera. On a verified completion, the camera then deletes the video off of the device. On a failed transfer, the camera will restart the transfer from the beginning. If a camera is lost prior to uploading video, the video will not be able to be recovered remotely. If a camera is destroyed, forensic recovery methods can be attempted if the solid-state embedded media card is viable.

Ecom requires two-factor authentication to access the system. Inside the system, users can only access their own videos, via their account, as well as any subordinate's videos, established by group permissions. Every account log in and video viewing is logged. Videos are tagged and categorized according to context and sensitivity, for instance all videos of service of arrest warrants will be labeled as such, and videos that involve the use of force will be labeled as such, in addition. If an agent has to view a sensitive video multiple times, he or she is able to leave comments about why an abnormal level of attention is necessary. Administrators can limit the number of views possible for sensitive videos, and any sharing of videos with other Ecom users must be authorized by appropriate DEA personnel, as discussed above in Section 6.2. Individual users can edit a video, but the original copy is preserved. Videos uploaded cannot be deleted.

This video categorization capability will also allow for DEA to tailor disposal. Each type of evidence will be maintained in accordance with its related records schedule, and there is an additional 30-day period after the expiration of the retention schedule where videos are moved to a cache and cannot be completely deleted.

c. Potential Threats Related to Dissemination

There is a potential risk to privacy that could result from improper access and the potential unauthorized disclosure of the information within the BWC program. The information collected by the program may be shared within DEA, the Department, federal, state, local, tribal, and territorial agencies, as well as opposing counsel for purposes of criminal prosecutions. DEA mitigates these risks by using authentication tools and controlling access to information on a need to know basis. ECom requires a Multi-Factor Authenticator (MFA) for users to log in. Additionally, DEA is working to incorporate

OKTA[1] as an additional MFA. These disseminations are done consistent with DOJ policy and applicable laws and regulations. Further the disseminations are shared only with those authorized to receive them for legal and authorized purposes.

[1] Okta provides identity and access management solutions that enable organizations to securely implement multi-factor authentication to gain access to their networks and applications. See https://www.okta.com/.