Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

Privacy Impact Assessment
for the
Body Worn Camera Program

Issued by:
Adam Siple, Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 16, 2022

(May 2019 DOJ PIA Template)

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.)

Under the U.S. Department of Justice Body Worn Camera (BWC) policy, issued June 7, 2021, Department components, including the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), must develop and submit a BWC policy requiring special agents to wear and activate 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. This Department policy is in addition to the permitted use of BWCs when task force officers (TFO) are employed by a law enforcement agency that mandates the use of body worn cameras (BWCs) on federal task forces.

ATF uses the Axon Enterprise, Inc. (Axon) owned website, Evidence.com, as the Software-as-a-Service (SaaS) central repository for evidence collected by BWCs and other sources of digital media. [1] The system is Federal Risk and Authorization Management Program (FedRAMP)[2] certified and Joint Authorization Board (JAB)[3] approved. Evidence.com leverages a FedRAMP-authorized Infrastructure-as-a-Service (IaaS) at the FedRAMP High impact level.[4]

Evidence.com serves two purposes for the ATF BWC Program: 1) it enables ATF special agents to store audio and video recordings and associated metadata from their own BWCs; and 2) it enables federally deputized task force officers (TFOs) and Special Deputies (SD)[5] to share audio and video recordings and associated metadata from BWCs worn during the serving of planned arrest warrants, other planned arrest operations, and during the execution of search warrants with ATF. Evidence.com provides a Partner Application Programming Interface client application (application), which ATF special agents – and eventually, other appropriate ATF and task force personnel – use for their own BWC evidence and case management, as well as to receive information from TFOs. Application users can request access to BWC data, create case files, read or review BWC evidence, and update case-related assignments.

---

[1] Other digital media includes, but is not necessarily limited to photos, audio recordings of 911 calls, screenshots and recordings of mobile phones, and other digital files received from partner law enforcement agencies. The processing of other digital media by Evidence.com will be documented separately from the Body Worn Camera Program.
[2] The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. See https://www.fedramp.gov/.
[3] The JAB is the primary governing body for FedRAMP and includes the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA). See https://www.fedramp.gov/jab-authorization/.
[4] The FedRAMP high impact level is the standard for security necessary to protect the federal government's most sensitive, unclassified data in cloud computing environments. Certification is based on compliance with 421 system controls which are applied for the integrity and safeguarding of the system and data.
[5] Task Force Officers (TFOs) are ATF agents who are temporarily assigned to a task force. Special Deputies (SDs) are sworn state, county, or local law enforcement officers assigned an ATF task force on a part time basis and whose department has a fully executed task force memorandum of understanding on file with ATF.

Within the scope of this PIA, the information processed and stored in Evidence.com includes audio and video recordings taken by the BWCs and associated metadata. In this case, metadata includes information about the footage that helps ATF understand and manage the video, such as notes, clips, markers, and audit trails. Notes are, in fact, notations entered to provide details on what the footage depicts. Clips are smaller extracted sections of a video; for instance, a 30-second "clip" of a longer video recording. Markers are mechanisms to flag certain sections of the video and are useful for indicating an important event so that users can easily find the event when replaying the video. Finally, audit trails show events and changes related to the footage; this may include information such as the device type and serial number of the BWC and any associated devices (e.g., the camera, helmet mounted camera and controllers) and information about which users have accessed the footage.

While the ATF BWC Program data in Evidence.com is stored on the cloud site, and the cloud vendor provides the infrastructure and platform services, that vendor has no access to the data. ATF system administrators restrict access to approved users with an ATF workstation through single sign-on (SSO) authentication and access control lists that case agents manage to permit access to individual case data.

This PIA was prepared because the ATF BWC Program collects information in identifiable form relating to members of the public. As required by Section 208 of the E-Government Act of 2002, this PIA explains how such information is stored, managed, and shared, in accordance with Federal privacy and information protection guidelines.

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.

BWCs are an effective tool for law enforcement to ensure officer accountability and safety, to better defend or learn from their actions during a particular encounter, and to make departments more transparent. Video footage recorded by BWCs can also enable departments to collect evidence during investigations and conduct an "excessive force review" or Internal Affairs investigation, as needed. "Excessive force" refers to the use of force in excess of what a police officer would reasonably believe is necessary in situation. As described in Section 1, Axon's cloud-based application provides an easy user interface for ATF law enforcement agents and TFOs on task forces run by ATF who are using BWCs to record and manage digital evidence.

Evidence.com's SaaS delivery model allows for the management of BWC Program evidence without the need for local storage infrastructure or software. The delivery model consists of three core parts: capture, transport, and information management.

Capture refers to the action of recording information on physical BWC hardware worn by the special agents and TFOs. Special agents and TFOs record video on the BWC hardware during either 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 the execution of a search or seizure warrant or order.

Transport refers to the movement of evidence through the BWC "system," as a whole, which consists of the BWC camera hardware where the recording is initially captured, through the Axon Dock hardware, to the Axon Evidence Upload XT software application, and the Evidence Sync software application. The Axon Dock functions as the docking, charging, and upload station for Axon body worn cameras. Axon Evidence Upload XT is a Windows-based desktop application that enables users to easily upload digital evidence generated from non-Axon BWC hardware (when supporting agency personnel use other brands of BWCs) to their agency's Evidence.com account. Evidence Sync is a Windows-based desktop application that provides a secure interface for uploading and managing logs and videos captured by Axon and non-Axon BWCs.

Information management refers to the secure storage of the media within Axon using several encryption tools and protocols. Security safeguards include multiple levels of encryption for "Enhanced Video Authenticity & Integrity Validation" between the BWC and Axon Evidence Upload XT. First, "Secure Boot" ensures that the system only operates using software that is trusted by the manufacturer. "Disk Encryption" utilizes encryption software or hardware to encrypt every bit of information that goes on a disk or disk volume. Whole disk encryption encrypts (converts the data into unreadable code) the entire disk. The BWC "system," as a whole provides protection for information while at rest by encrypting all information at rest and in transit, preventing unauthorized access and data tampering, and ensuring all data comes from a verifiable and trusted source.

The actions a user can take in Evidence.com depend on the permissions granted to the user by the ATF administrator. Authorized users of Evidence.com will access the SaaS through an ATF workstation using an internet browser and single sign-on (SSO) authentication. Access to Evidence.com must traverse the Department's Justice Cloud Optimized Trusted Internet Connection Services (JCOTS) program. The JCOTS program provides several layers of network and application protection. These protections include logs of all activity associated with a connection to the service into an audit log or trail. This allows ATF to see who has accessed each case, and see errors related to failed logons or system failures. Also, ATF has data loss prevention services that restrict the flow of PII to external services or agencies. This includes breaking the encryption of traffic leaving the Department and re-encrypting after completing analysis. Finally, ATF requires that requests for information by non-DOJ entities be formally reviewed by the local ATF legal counsel for approval if appropriate, and that agencies with which ATF shares BWC data have memoranda of understanding (MOU)[6] in place outlining the responsibly of each agency.

Types of information processed and stored in the system include audio and visual recordings and associated metadata (e.g., notes, clips, markers, transcripts, and audit trails). This information collection could include audio and video of law enforcement activities and operations. Per DOJ policy, all BWC recordings made by special agents, or by TFOs or SDs during federal task force operations, are deemed federal records and the property of the federal agency sponsoring the task force. ATF employed contractors (e.g., paralegals) with a need for the digital recording would be granted access by the digital owner (case agent or their supervisor) to the case in Evidence.com. Neither ATF nor its associated users, including contractors, will not be able to amend the original recording. ATF users could, however, save copies of the recording, redact copies of the recording within Evidence.com, and

[6] A Memorandum of Understanding (MOU), is a type of agreement between two (bilateral) or more (multilateral) parties that outlines terms and details of a mutual understanding or agreement, noting each party's requirements and responsibilities.

save redacted clips of the recording as needed. All recordings and clips will remain within Evidence.com, and the audit trail will display all actions taken.

As a separate note, the cameras employed by ATF do not have facial recognition capabilities and Evidence.com is not being used to conduct facial recognition on the recordings.

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. § 599A. Bureau of Alcohol, Tobacco, Firearms, and Explosives • 28 CFR Subpart W - Bureau of Alcohol, Tobacco, Firearms, and Explosives • 18 U.S.C. Chapter 44, Gun Control Act • 26 U.S.C. Chapter 53, National Firearms Act • 22 U.S.C. Chapter 2778, Arms Export Control Act • 18 U.S.C. Chapter 40, Importation, Manufacture, Distribution and Storage of Explosive Materials • 18 U.S.C. Chapter 114, Contraband Cigarette Trafficking Act • 18 U.S.C. § 1952 Interstate Transport in Aid of Racketeering
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	• DOJ Policy, Use of Body-Worn Camera by Federally Deputized Task Force Officers (October 2020) • Memo from Deputy Attorney General Lisa Monaco, Body-Worn Camera Policy (June 2021) at https://www.justice.gov/oip/page/file/1332151/download

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
Name	X	A, B, C & D	**DOJ/ATF and other Federal employees, and detailees (A&B)** Names of any law enforcement personnel involved the event that could be listed in the warrant, and possible names of individuals in the area of operation could be recorded. **Members of the public (citizen, USPERs or non-USPERs) (C&D)** Names of suspect(s), which will be listed in the warrant, and possible names of individuals in the area of operation could be recorded.
Date of birth or age	X	C & D	**Members of the public (citizen, USPERs or non-USPERs) (C&D)** Age or DOB for suspect(s), which will be listed in the warrant, and possible ages of individuals in the area of operation could be recorded.
Place of birth			
Gender	X	A, B, C & D	Gender of individuals may be disclosed or evident within audio or video recordings of anyone at the scene, within the parameters set forth by the Department of Justice.
Race, ethnicity or citizenship	X	A, B, C & D	Race information may be disclosed or evident within audio or video recordings of anyone at the scene, within the parameters set forth by the Department of Justice.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			

(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
Driver's license	X	C & D	Suspects or others on-site, including witnesses, could be asked to show identification in the area of operation which could be recorded. While DOJ policy states that BWCs should be turned off during this process, incidental collections may occur.
Alien registration number	X	D	Suspects or others on-site, including witnesses, could be asked to show identification in the area of operation which could be recorded.
Passport number	X	D	Suspects or others on-site, including witnesses, could be asked to show identification in the area of operation which could be recorded.
Mother's maiden name			
Vehicle identifiers	X	A, B, C, & D	Vehicles and occupants will be recorded to the extent they exist in the area of operation.
Personal home address	X	C & D	There is no field for this subject, but it could be included in a video recorded (house next door may be recorded).
Personal e-mail address	X	C & D	There is no field for this subject, but the information may be included in a contact detail from a suspect or witness and added as supplemental information by agent.
Personal phone number	X	C & D	There is no field for this subject, but the information may be included in a contact detail from a suspect or witness and added as supplemental information by agent.
Business address	X	C & D	There is no field for this subject, but it could be included in a video recorded (business next door may be recorded).
Business e-mail address	X	C & D	There is no field for this subject, but the information may be included in a contact detail from a suspect or witness and added as supplemental information by agent.
Business phone number	X	C & D	There is no field for this subject, but the information may be included in a contact detail from a suspect or witness and added as supplemental information by agent.
Medical records number			

(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
Medical notes or other medical or health information	X	A, B, C & D	Injuries may be disclosed or evident within audio or video recordings of anyone at the scene.
Financial account information			
Applicant information			
Education records			
Military status or other information	X	C & D	Military-related information or items, such as uniforms, may be disclosed or evident within audio or video recordings of anyone at the scene.
Employment status, history, or similar information	X	A, B, C & D	Employment-related information or items, such as uniforms, may be disclosed or evident within audio or video recordings of anyone at the scene.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents	X	C & D	Arrest warrants or search warrants may be disclosed or evident within audio or video recordings of anyone at the scene.
Device identifiers, e.g., mobile devices	X	A & B	Serial numbers of BWCs, and the make and model of devices used will be stored in Evidence.com.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Arrests and charge information will be recorded. Past criminal acts (criminal history) may also be disclosed or evident within audio or video recordings of anyone at the scene.
Juvenile criminal records information	X	C & D	Juvenile records related to a subject of the warrant maybe included, as could information disclosed within audio or video recording by anyone at the scene.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, & D	Violations to civil law may also be disclosed or evident within audio or video recordings of anyone at the scene.
Whistleblower, e.g., tip, complaint or referral	X	C & D	Tips, whistleblower complaints or information, or comments and referrals related to investigations may be disclosed or evident within audio or video recordings of anyone at the scene.
Grand jury 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
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C & D	Information concerning witnesses, or information related to investigations may be disclosed or evident within audio or video recordings of anyone at the scene.
Procurement/contracting records			
Proprietary or business information	X	C & D	Proprietary or business information may be disclosed or evident within audio or video recordings of anyone at the scene.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C & D	While in use, BWCs have GPS location tracking enabled to ensure the safety of officers and others at the scene.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, & D	BWCs are video recording equipment. Photographic stills may be captured of anyone or anything at the scene.
- **Video containing biometric data**	X	A, B, C, & D	BWCs are video recording equipment. Video recordings may be captured of anyone or anything at the scene.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, & D	BWCs are audio recording equipment. Video recordings may be captured of anyone or anything at the scene.
- **Scars, marks, tattoos**	X	A, B, C, & D	Scars, marks, and tattoos may be disclosed or evident within audio or video recordings of anyone at the scene.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	Axon users will use User IDs to access the application.
- **User passwords/codes**	X	A	Axon users will use passwords and codes to access the application.
- **IP address**	X	A	Axon will collect the IP address of users during access to the application.
- **Date/time of access**	X	A	Axon will collect the date and time of user access to the application
- **Queries run**	X	A	Axon will collect the queries run by users within the application.

(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	Axon will collect the content of files accessed by users within the application.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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	X
Phone		Email			
Other (specify): Audio and video recordings of individuals are captured in person. System access and auditing information of Axon application users is logged while users are online.					

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): Audio and video recordings gathered by ATF special agents and TFOs under the auspices of ATF or ATF-controlled investigations using BWCs are uploaded to the Axon application via a secure logon.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Some information will be collected from members of the public whose likenesses or voice are captured using BWCs.					

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	Supervisors will have access to all information collected from special agents assigned to their group as well as information received for TFO's assigned to their groups. Assistant Special Agents in Charge (ASAC) and Special Agents in Charge (SAC) will have access to the information for the entire division, including the capability to review for an excessive 'Force Review' or an Internal Affairs investigation as needed. This could occur either through direct access to Axon or a digital file extracted from Axon.
DOJ Components	X	X		Since all information in Axon is stored in a FedRAMP approved cloud, ATF will be able to share digital data, and audit trails or logs with other DOJ components outside ATF as lawful and appropriate. Authorized Axon application users will be able to send a partner an invite to the information through the Axon share function. ATF partners with the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), United States Attorneys' Offices (USAOs), and the United States Marshals Service (USMS) in cases with joint jurisdiction. Memoranda of Understanding (MOUs) are in place authorizing the sharing of information.

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		X	ATF follows existing procedures to share information from the Disclosure Documentation and Handling of Investigative Information (ATF O 3270.10D). This requires a Disclosure Memo to be submitted between ATF and partner law enforcement agencies which will outline details for the use of BWCs by TFOs consistent with laws, regulations, policies, and procedures and that the recordings deemed to be federal records are subject to federal retention and information access requirements. Federal agency recipients who do not have an Evidence.com logon can receive case data from the case agent who will provide a link to a download site with no logon required. Only the files requested will be available. Permissions are set by the agent to allow the file(s) to be shared, downloaded, or just viewed, as well as the audit trail and transcript and the date range for the data availability. Agencies that have an account can be provided access via a partner share, by the case agent adding the recipient to the access list for the case files. Recipients will not receive access to any other ATF information stored in Evidence.com.
State, local, tribal gov't entities	X		X	State, local, or tribal government entities requesting BWC Program evidence from ATF shall follow the process from Disclosure Documentation and Handling of Investigative Information (ATF O 3270.10D), requiring a

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.**
				memorandum of understanding (MOU) for joint missions, and a Disclosure Memo outlining the details for the event the BWCs were used for and requirement for data to be submitted ATF. TFO members originating with state, local, or tribal entities that have Evidence.com accounts will be able to access their audio and video recordings, when records from other agents are required the case agent or their supervisor can grant access by adding the requestor to the access list. Requestors who do not have an Evidence.com logon can receive the case data from the case agent who will provide a link to a download site with no logon required, where only the BWC Program files requested will be available. Permissions are set by the agent to allow (or not) the file(s) to be shared, downloaded or just viewed, as well as the audit trail and transcript and the date range for the data availability.
Public	X			Members of the public can submit a Freedom of Information Act (FOIA) request for audio and video recordings captured by BWC. In appropriate instances, recordings from Evidence.com may be released to the public, after redaction of all sensitive materials or images. In order for local authorities (TFOs), to release information, ATF must review and grant approval.

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			When recordings captured by BWC are evidentiary in value, the recordings are logged in and treated as all other evidence is and is provided to counsel, courts, or other judicial tribunals as part of the discovery process. In order for information from Evidence.com (digital data, and audit trails or logs) to be released, a request would be made to ATF legal counsel who must review and grant approval.
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.

Any information that resides in Axon is processed and disseminated in accordance with legal requirements, federal regulations, and Department policy. ATF provides only statistics and case filings to the "Open Data" site (www.data.gov).

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.

The following ATF and DOJ SORNs provide generalized notice to the public:

JUSTICE/DOJ-002 Department of Justice Information Technology, Information System, and Network Activity and Access Records; 86 FR 132 (7-14-2021).

JUSTICE/ATF-003 Criminal Investigation Report System, Exemptions Claimed Pursuant to 5 U.S.C. 552a (j)(2). See 28 C.F.R. § 16.106., 68 FR 3551, 553 (1-24-03) (last published in full),

82 FR 24147 (5-25-2017).

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.

Individual consent is not sought when audio and video recordings are made during the execution of lawful warrants; when charges result, the recordings become part of the evidence in a case and are retained according to legal requirements.

When required by law, ATF provides data subjects with appropriate notice of information collection under the Privacy Act, 5 U.S.C. § 552a(e)(3). For instance, ATF agents are provided with notice when asked for their badge number, email, and the group they are working with, when they request access to the system.

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.

ATF follows Department procedures regarding requests for access to, or amendment of, records pertaining to an individual, including those maintained within a system of records in accordance with the Privacy Act. See https://www.justice.gov/opcl/doj-privacy-act-requests. Privacy Act requests for access to records are processed under both the Privacy Act and the Freedom of Information Act (FOIA/PA), 5 U.S.C. § 552. All such requests are submitted to ATF's Information and Privacy Governance Division for processing and response.

Amendments and corrections cannot be made to the original audio or video recordings. The original recordings captured in Axon are an official record of an event. Changes can only be made to copies of the original recordings pursuant to strict requirements indicated elsewhere in this PIA to maintain the integrity of the data originally recorded regarding the audio, video, and metadata of the live event.

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):** Granted: 12/18/2020 Expires: 12/18/2023

	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:** ATF has an outstanding POAM to better support audit review and analysis: ATF will export audit logs to a Splunk[7] solution via the Axon reporting tool application programming interface. As a compensating control if Splunk log implementation cannot be completed, individual audit reports can be generated through Axon console, and accessed by ATF personnel via the Axon FedRAMP environment on the ATF Network.
	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:** Axon has completed all required security and functional testing and evaluation in accordance with Department IT development procedures. Additionally, it has undergone a full security assessment in accordance with the DOJ Security and Privacy Assessment and Authorization Handbook. Axon operates within the boundary of ATF's primary infrastructure environment, where it is subject to full system monitoring and auditing in accordance with ATF and Department guidelines. Users must be on (or in) the ATF network and access ATF Evidence.com from the cloud. Users cannot access ATF's instance of Evidence.com from any network other than the ATF's. All system documentation supporting these activities are maintained within the Department's system of record, Cyber Security Assessment & Management (CSAM) tool.
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:** Axon provides analytic and auditing tools for the management of system users and events, such as monitoring system usage, keeping track of what videos have been uploaded and who has reviewed or shared, and files are set for deletion by records schedule requirements. Axon audits access and use at multiple layers, including the network and application processing levels. All logs are generally reviewed on a weekly basis by onsite administrators and then gathered and centrally managed using the Department's audit analysis solution, Splunk. All logs are forwarded to the Justice Security Operations Center (JSOC) for automated analysis and review.

[7] Splunk captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

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.** ATF contractors are provided the same annual privacy training as all ATF employees, and those with greater access receive additional training about the protection of PII**.** All contractors are required to sign the DOJ General or Privileged Rules of Behavior, as determined by their role. All associated IT related contracts within ATF are required to comply with the policies and guidelines defined and documented within the Department of Justice Procurement Guidance Document 15-03, Security of Information and Information Systems, and the Acquisition Policy Notice 2021-07A.
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:** All ATF users are subject to organizational and Department annual computer security awareness and privacy specific training, which includes acknowledgment of the DOJ General or Privileged Rules of Behavior, as appropriate. In addition, personnel who have specific administrative roles within the application require and have received specialized role-based training, both prior to starting their position and as needed.

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?

Access to the Axon application is limited to authorized ATF account holders, and is based on operational requirements. ATF system administrators will configure each account to customize the user's permissions after determining what files are needed.

The administrators can also give access to an Axon add-on functionality known as "redaction assistant," which checks videos for common objects, such as license plates, mobile data terminal or mobile digital computer screens, and faces. Redaction assistant automatically generates a copy of the recording that masks those objects to remove the personally identifiable information without altering the original recording.

Additionally, audio and video recordings are not accessible from the BWCs themselves; the information must be uploaded to a docking station in order to be accessed. Information is protected from interference by encryption during transmission to, and at rest on the Axon application.

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 of information is dependent on investigatory and prosecutory requirements, as well as federal records retention requirements. Once a case is adjudicated and closed, disposition instructions for the associated information are set up in Axon to automatically delete the information at the appropriate time.

Requirements governing retention and disposition of ATF documents and information are documented within ATF Records Control Schedule 1340.7, recordings are covered under item #3351 Criminal Case Files (Investigative Files). The ATF records schedule is consistent with National Archives and Records Administration regulations and rules.

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:

JUSTICE/DOJ-002 Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 132 (7-14-2021).

JUSTICE/ATF-003 Criminal Investigation Report System, Exemptions Claimed Pursuant to 5 U.S.C. 552a (j) (2). See 28 C.F.R. § 16.106., 82 FR 24147 (5-25-2017).

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The privacy risks associated with information collected by the ATF BWC Program primarily relate to the loss of confidentiality and integrity of the information. Access by unauthorized entities to sensitive

information, including personal information collected for investigation or litigation could lead to destruction or corruption of that information, compromised identities, exposure of sensitive records and personal information which could be used to harm individuals, and disruption to an ongoing investigation or litigation.

To mitigate this risk, access to Evidence.com is limited to authorized ATF account holders and is based on operational requirements using Access Control Lists (ACLs). ACLs are implemented and maintained by each case agent and system administrator, the agent is placed in the ACL for their work group which provides access to their direct supervisor and department chief, the agent can then grant access to individuals as the case requires. Access to the BWC devices does not automatically grant access to the data contained within, the data can only be accessed with a docking station and then the data will only be uploaded and available to the ATF user the device is assigned to.

Users are required to use a single sign-on (SSO) authentication method to securely authenticate their accounts through a PIV card and government issued laptop, and must be connected to the ATF network directly or via a virtual private network (VPN). Evidence.com integrates its access control with the ATF Active Directory for streamlined and secure user management. Additionally, audit logs are created to record which users have accessed the system, what information is accessed, and the date and time of access. These logs are read-only and can only be reviewed by the information owner (each agent or TFO is considered an information owner) or the system administrator. As an added layer of security, Evidence.com enforces session timeout after 10 minutes of inactivity.

Information is protected from accidental deletion with a deletion protect setting, which requires approval from the information owner. Prior to a file deletion, notification emails are sent to the information owner. There is also a deletion remorse period set by the information owner, during which the information owner can recover deleted evidence files.

When information is shared with other agencies, access is given through a partner share function which is only available through an invitation sent from an ATF user. When information is being released to state and local prosecutors, the ATF division legal counsel is notified by the special agents or TFOs per the ATF standard operating procedures (SOP) for Digital Evidence Management. Requests for information by non-DOJ entities must be formally reviewed by the local ATF legal counsel for approval if appropriate, and that agencies with which ATF shares BWC data have memoranda of understanding (MOU) in place outlining the responsibly of each agency.

Another privacy concern is that ATF will collect more information on members of the public than is necessary. BWCs are capable of capturing primary evidence in a manner that portrays a compelling and indisputable account of an incident. The use of BWCs is a prime example of a technology which, by design, could collect information about people in private and semi-private places who are going about their lives as agents and subjects move around them. To some degree, this is inevitable, because a microphone and camera are non-discriminatory and capture all audio and video within their vicinity. To safeguard against capturing excessive audio or video about non-subjects, DOJ policy regarding Use of Body-Worn Cameras by Federally Deputized Task Force Officers stipulates the following (along with certain exceptions elsewhere in the policy): TFOs employed by a law enforcement agency that mandates the use of BWCs on federal task forces may wear and activate their recording equipment for the purpose of recording their actions during task operations only during: (1) a planned attempt to serve an arrest warrant or other planned arrest; or (2) the execution of a search warrant. 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 federal supervisor on the scene as designated

by the sponsoring federal agency. DOJ policy also restricts the recording of undercover personnel, informants and on-scene witnesses, personnel utilizing specialized or sensitive equipment or techniques, and on-scene actions by non-law enforcement personnel assisting at the scene or event. Should either a person who is not relevant to the case, or an undercover agent or other sensitive individual be recorded, their image may be redacted from copies while maintaining the integrity of the original recording.

To prevent the unauthorized access to, use of, or disclosure of any incidentally collected information, the Axon BWC hardware and software, docking and uploading hardware and software, and Evidence.com all use several encryption tools to protect the information at rest in the system and when information is in transmission.

Hash Trees are used to prevent unauthorized access to information by checking for inconsistences in the information that is stored and transferred in the system. The output is unique for every input and can be considered as a type of "fingerprinting", each change to a data block will also have a unique fingerprint. During transmission of data blocks the received hash tree is checked against the trusted top hash stored in the system, and if the hash tree is damaged or fake the transmission will fail. Hash trees are used to verify data quickly. Hash trees are effective because they use hashes rather than complete files and the hashes are much smaller than the original file. When Hash Tree is implemented, it facilitates multiple layers of forensic integrity.

ATF case agents also have the ability to utilize the "redaction assistant" feature to mask unnecessary PII of the public that was inadvertently captured during a mission. As described earlier, all original digital recordings will remain intact, even when masking or redacting is implemented. The original recording will remain unchanged, any deleted files have a seven-day grace period that allows the system administrator to restore the file in full. Regardless, audit logs will be retained of all actions taken with respect to the BWC Program data.

Finally, retention and maintenance of audio and video recordings and associated metadata will depend upon legal and policy requirements of the given investigation, operation, litigation, or other circumstances such as oversight matters.