Template Version Number: 01-2021

U.S. Department of Commerce
Bureau of Industry and Security

Privacy Impact Assessment
for the
Body Worn Camera (BWC) Program

Reviewed by: Keven Valentin, Bureau Chief Privacy Officer

■ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.07.01 14:58:56 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Bureau of Industry and Security (BIS) / Body Worn Camera Program

Unique Project Identifier: 000552000

Introduction: System Description

Provide a brief description of the information system.

On May 25, 2022, President Joseph R. Biden, Jr. issued Executive Order (EO) 14074 on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*. In accordance with EO 14074, the United States Department of Commerce (DOC) Bureau of Industry and Security (BIS) Office of Export Enforcement (OEE), hereafter referred to as BIS OEE, intends to implement a Body Worn Camera (BWC) program requiring Special Agents (SAs) 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; (2) the execution of a search or seizure warrant or order; or (3) other missions assigned by the OEE Director. BIS OEE intends to use the Axon Enterprise, Inc. (Axon) Cameras and Axon owned website, Evidence.com, as the Software-as-a- Service (SaaS) central repository for evidence collected by BWCs. The system is Federal Risk and Authorization Management Program (FedRAMP) certified and Joint Authorization Board (JAB) approved. Evidence.com leverages a FedRAMP-authorized Infrastructure-as-a-Service (IaaS) at the FedRAMP High impact level.

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 an SA's camera. The SA 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 SAs and their designated, pre-authorized supervisors to view the video footage and create a written transcript of audio collected from the video.

This PIA was prepared because the 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.

(a) Whether it is a general support system, major application, or other type of system

This is a major application.

(b) System location

The system used by BIS OEE is located at Microsoft's Azure Government Cloud in the Eastern Region, with backup located in Microsoft Azure Government Cloud in the Central Region. Both regions employ consistent and identical security policies, protocols and controls which are all

controlled and maintained as part of the Axon FedCloud FedRAMP authorization.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Standalone system accessed through the BIS infrastructure and supports the law enforcement activities for the Commerce USXPORTS Exporter Support System.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Axon BWCs collect video in 720p 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 BIS OEE SA. 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. The cameras do not have facial recognition capabilities or any other biometric collection or analysis capabilities.

(e) How information in the system is retrieved by the user

Authorized user accounts have access to their own recordings via the web portal or desktop application. Administrative access is required to view other content and/or activity created by other users. Administrators have access to all recordings and the authority to change user permissions. All other users do not have direct access to recordings other than their own.

(f) How information is transmitted to and from the system

BIS OEE policy requires SAs to upload camera footage within 72 hours of capture. To upload the camera footage, Evidence.com requires a "handshake" double key authentication with the server, which is done by docking the camera via physical connection with an Axon dock station that has a proper mobile or hard-wired internet connection, or via USB to a BIS OEE 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 BIS OEE workstation or laptop. Once this is done, the video starts to transfer, sending smallest files first and working its 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 from 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.

(g) Any information sharing

Information will be shared within BIS on a case-by-case basis and direct log-in access as necessitated for law enforcement or training purposes. Information may also be shared with other DOC bureaus, federal agencies, state/local/tribal government agencies, or counsel, courts, or other judicial tribunals as needed in support of a law enforcement matter or for litigation purposes.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- 15 CFR § 758.7;
- The Export Control Reform Act (ECRA) of 2018 (Section 1761(h)), formerly known 12c of the Export Administration Act (EAA) and the Denied Persons List or Export Enforcement laws and regulations are adhered to when collecting information for investigative purposes.
- Executive Order (EO) 14074 on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety.*

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

FIPS 199 Categorization – High

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__X__ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License	X	j. Financial Account	
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration	X	l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
**Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form*: BIS is not actively collecting SSNs. If SSN information is collected it is being collected as part of the scene as the agent is carrying out official duties while wearing an activated BWC.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	X
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos	X	k. Signatures	
b. Palm Prints		g. Hair Color	X	l. Vascular Scans	
c. Voice/Audio Recording	X	h. Eye Color	X	m. DNA Sample or Profile	
d. Video Recording	X	i. Height	X	n. Retina/Iris Scans	
e. Photographs	X	j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

BIS OEE implements Axon's Body Worn Camera FedRAMP authorized Software as a Service (SaaS) solution, to gather and preserve evidence during the specified field operations as outlined in the BIS OEE BWC Policy, such as the execution of search and arrest warrants, including during interviews with arrestees or detainees that take place during enforcement operations, and to use for training purposes in support of BIS OEE investigations.

Video and audio recordings captured through a BWC is uploaded to Axon's platform, Evidence.com, to which OEE SAs and support staff have limited access. Recordings may be used as evidence in OEE investigations as well as for OEE training purposes.

Evidence.com's SaaS delivery model allows for the management of 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 SAs. BWC videos are captured during either a preplanned attempt to serve an arrest warrant or other pre-planned arrest, the execution of a search or seizure warrant or order, or other missions assigned by the OEE Director.

Transport refers to the movement of evidence through the BWC "system,", 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.

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 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," 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 BIS OEE administrator. Authorized users of Evidence.com will access the SaaS through a secure BIS workstation using an internet browser and SSO authentication. To log into Evidence.com, users must enter an assigned 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. Evidence.com accomplishes this by group permissions and has monitoring and auditing controls to view all user activities in the system. The audit log created by the application detects inappropriate copying or sharing of the video. Any action involving the video (upload, viewing, exporting, etc.) is logged in the audit trail. Video can also be shared with other components that are using Evidence.com, though BIS OEE 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 BIS OEE 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.

The system used by BIS OEE is located at Microsoft's Azure Government Cloud in the Eastern Region, with backup located in Microsoft Azure Government Cloud in the Central Region. Both regions employ consistent and identical security policies, protocols and controls which are all controlled and maintained as part of the Axon FedCloud FedRAMP authorization. The FedRAMP Authorization process has a full set of criteria and requirements for how all PII and Sensitive Personal Information (SPI) are supposed to be handled and maintained to obtain the FedRAMP Authority to Operate. Axon FedCloud operates in a posture where the actual system being utilized writes full backups to a backup site daily and has hourly backups of the changes sent to the backup site also. The backup site can be made ready to use as the primary site in the event of some type of emergency where the primary site is unresponsive to users in less than 12 hours. In the event of needing to bring the backup site up to be the primary site, Axon would work with BIS OEE to do so and validate the integrity of the backup site and data to make sure the PII is fully in tack and correct.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify): Body Worn Cameras			
	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.		

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The BWC program will record official law enforcement encounters except when doing so may jeopardize a SA's safety. 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.

Information recorded by BWC may include:

Name; Date of Birth or Age; Gender; Race, Ethnicity, or Citizenship; Driver's License; Alien Registration Number; Passport Number; Vehicle Identifiers; Personal Home Address; Personal E-mail Address; Personal Phone Number; Business Address; Business E-mail Address; Business Phone Number; Medical Notes or other Medical or Health Information; Military Status or other Information; Employment status, History, or Similar Information; Legal Documents; Device Identifies (i.e. mobile devices); Criminal Record Information; Juvenile Criminal Record Information; Civil Law Enforcement Information; Whistleblower; Vehicle License Plate Number, Vehicle identifiers VIN, Certificate/Driver's License numbers* - Used for identifying vehicle owners. Internet Protocol (IP) Address Numbers, User ID, User passwords/codes – Information to access internet and intranet resources. Medical Records, Medications, Medical notes or other medical or health information – Used for investigative purposes. Military History/Service Connection, Duty Station – Used for identifying individuals and investigative purpose.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The privacy risk associated with sharing data within the BIS OEE is that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Additionally, over collection by an agent in the field is an associated privacy concern.

Controls to mitigate these risks include Access restrictions to authorized officials; Only authorized use of information shared; Limits on uses and additional sharing; Maintaining retention periods or return of information shared, data destruction as well as utilizing Secure File Transfer Protocols for transmission of information. Further, strict policy on what activities can and must be recorded, which users must read and adhere to, are present. 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 BIS OEE will not utilize the system's automatic on/off switch or its live streaming feature.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		X
DOC bureaus	X		
Federal agencies	X		X
State, local, tribal gov't agencies	X		
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Counsel, courts, or judicial tribunals for litigation purposes	X		
	The PII/BII in the system will not be shared.		

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
X	Yes, notice is provided by other means.	Specify how: BIS OEE cameras worn by SAs will be positioned in obvious places on the criminal investigators without compromising the criminal investigator's safety so that the public can visually determine if a criminal investigator is using a camera, as follows: • If a tactical vest (body armor) is worn, the camera will be worn on the outside/front of the body armor. Body armor is worn over the criminal investigator's clothing or helmet. • In the event a camera is deployed when body armor is not worn, the camera will be secured to the criminal investigator's outer clothing, lanyard, or belt. Cameras also have indicator lights that indicate when they are recording.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:

X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Due to the purpose and nature of the system, to support law enforcement operations and investigations, individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. 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. Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements as circumstances mandate, when a juvenile is involved, or as stipulated by policy.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Due to the purpose and nature of the system, to support law enforcement operations and investigations, individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. 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. Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements as circumstances mandate, when a juvenile is involved, or as stipulated by policy.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: In all circumstances, BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings. BWC recordings will also be treated as potential evidence in a federal investigation subject to applicable federal laws, rules, chain of custody requirements, and policies concerning disclosure. All FOIA and Privacy Act procedures are handled by the BIS Office of the Chief Financial Officer and Director of Administration (OCFO/DOA). All requests for BIS OEE recordings unrelated to a pending criminal investigation or case will be forwarded to the Office of the Chief Counsel for Industry and Security (OCC-IS) for consult. System data will be made available to BIS OCC-IS as needed. In any situation where BWCs record content that otherwise should not be shared because of law enforcement sensitivities or privacy concerns, which could include activities involving classified information, undercover personnel, confidential sources, sensitive investigative techniques or equipment, minors, injured or incapacitated individuals, or sensitive locations such as restrooms, locker rooms, or medical facilities, the BWC Program Manager, in consultation with the BIS OCIO, and OCC-IS, may use redaction software to blur images or portions of images, or minimize audio content, when making copies of BWC recordings for any authorized purpose.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to Evidence.com requires username, password, and multifactor identification to gain access. Once access is granted, all actions taken within the system are tracked and viewable in an audit report accessible by the system administrators. Administrators can remove or suspend users when they leave the agency or when exigent circumstances exist. Additionally, 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.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. This is a new system. The A& A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The Axon Security Team is responsible for implementing the appropriate physical and technical safeguards to prevent unauthorized access to the system, including Evidence.com and related mobile applications. Noted security features include, without limitation, transport layer security encryption, AES 256-bit encryption, role-based user security, watermark screenshots, firewall compatibility, and a password-protected meeting option. This ensures that the recordings and associated data is encrypted in transit and while at rest. It is Axon's responsibility to collect and monitor the system's audit logs to ensure the system has not been hacked or otherwise compromised. Authorized user accounts have access to their own recordings via the web portal or desktop application. Administrative access is required to view other content and/or activity created by other users. Administrators have access to all recordings and the authority to change user permissions. All other users do not have direct access to recordings other than their own. This system is an implementation of the FedRAMP authorized, Axon 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). BIS OEE, specifically the System Owner in consultation with the Information System Security Officer, reviews the cloud service providers (CSP) provided audit logs for indications of inappropriate or unusual activity for both privileged and general OEE users of the system.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

___ Yes, the PII/BII is searchable by a personal identifier.

_X_ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
X	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. BIS-1, Individuals Identified in Export Transactions and Other Matters Subject to BIS Jurisdiction.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Information generated from the BWC Program will either directly or indirectly identify an individual.
X	Quantity of PII	Provide explanation: Information generated from the BWC Program may include large quantities of PII including an individual's name; date of birth; gender; race, ethnicity or citizenship; driver's license; alien registration number; passport number; vehicle identifies; personal address or other related PII; video containing distinguishing feature(s); and voice recording.
X	Data Field Sensitivity	Provide explanation: The system may maintain Sensitive PII such as date of birth; Driver License; or SSN.
X	Context of Use	Provide explanation: The data collected is for official law enforcement purposes, in accordance with President of the United States (POTUS) Executive Order 14074. Axon enables cloud-based workflows for digital evidence management, situational awareness, and records management to support the operational needs of agencies. Axon FedCloud operates as an isolated region of Axon Cloud Services that is dedicated to the US Federal community.
X	Obligation to Protect Confidentiality	Provide explanation: The Export Control Reform Act (ECRA) of 2018 (Section 1761(h)), formerly known 12c of the Export Administration Act (EAA) and the Denied Persons List or Export Enforcement laws and regulations are adhered to when collecting information for investigative purposes.

X	Access to and Location of PII	Provide explanation: Access is restricted by a role-based and least privilege principles. Access to the evidence management system requires an active BIS email account. Law enforcement officials require supervisor authorization to establish user accounts to access the system. Users will not have access to all data, they will have access to the data required to perform their duties based on their roles. Axon personnel undergo an extensive background check process to the extent legally permissible and in accordance with applicable local labor laws and statutory regulations. Axon personnel supporting Axon Cloud Services are subject to additional role-specific security clearances or adjudication processes, including Criminal Justice Information Services background screening and national security clearances and vetting. BIS stores BWC recordings uploaded by BIS OEE SAs using secure storage methodologies (on a cloud-based digital evidence platform accessed through the DOC network) with appropriate role-based access controls within an access-restricted federal facility that meets DOC security requirements. BIS utilizes a FedRAMP-authorized, SSO enabled, cloud-based SaaS application to store and manage video and audio files/data. Access to the audio/video data on the cloud application requires a user verification, consisting of BIS application-level security. BIS application security is controlled by both the vendor software application and Operating System Level security setting. BIS enhances security by limiting initial access and management of recorded data. Accordingly, BIS OEE users will not be allowed to delete or modify any uploaded data. Users will have the ability to upload data, add case log notes, and save the respective files in the system. Viewing, editing, deleting, exporting, and other permissions related to video and metadata rests with the BIS OEE application administrator.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The privacy risk associated with sharing data within the BIS OEE is that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Additionally, over collection by an agent in the field is an associated privacy concern. Controls to mitigate these risks include Access restrictions to authorized officials; Only authorized use of information shared; Limits on uses and additional sharing; Maintaining retention periods or return of information shared, data destruction as well as utilizing Secure File Transfer Protocols for transmission of information. Further, strict policy on what activities can and must be recorded, which users must read and adhere to, are present. 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 BIS OEE will not utilize the system's automatic on/off switch or its live streaming feature.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.