Affects Members Of the Public? X

Department of Energy

Privacy Impact Assessment (PIA)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	April 21, 2023
Departmental Element & Site	Office of Inspector General, Headquarters Operations
Name of Information System or IT Project	US Axon FedCloud
Exhibit Project UID	019-000001322
New PIA x **Update**	

	Name, Title	Contact Information Phone, Email
System Owner	Jeffrey Burnett Tech Ops Special Agent Headquarters Operations	202-705-4639 jeffrey.burnett1@hq.doe.gov
Local Privacy Act Officer	Alexander Borman Attorney-Advisor	202-586-1653 alexander.borman@hq.doe.gov
Cyber Security Expert reviewing this document (e.g.	Kshemendra Paul	kshemendra.paul@hq.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

ISSM, CSSM, ISSO, etc.)	Assistant Inspector General Cybersecurity Assessments and Data Analytics	
Person Completing this Document	Jeffrey Burnett	202-705-4639 jeffrey.burnett1@hq.doe.gov
Purpose of Information System or IT Project	Executive Order 14074 (E.O. 14704) "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," dated May 25, 2022, requires that Federal Law Enforcement Agencies (FLEA) issue policies for use of Body Worn Cameras (BWC) during appropriate circumstances, to include during searches and arrests. E.O. 14704 further requires FLEA to develop BWC policy with requirements that are equivalent to or exceed the requirements in the US Department of Justice BWC policy. US Department of Energy, Office of Inspector General (OIG), Office of Investigations (OI) policy requires Special Agents (SAs) actively participating in the execution of planned enforcement operations to wear and activate OIG-issued BWCs during the tactical portion of enforcement operations where the use of force may reasonably be anticipated. For the purposes of this policy, planned enforcement operations include the execution of search warrants and arrests and arrestee transport. BWCs may also be activated during interviews of subjects when deemed appropriate by the SA to capture the interaction or as requested by DOJ. BWCs will be activated by all participating OI SAs upon approaching a subject or premises during an enforcement operation and remain active until enforcement activities are completed, such as the securing of a search scene or securing and search of subjects. The use of BWC is not intended to be used during the actual search of a legally authorized premises after interactions with individuals have concluded and the premises has been deemed safe. OI Policy establishes the specific timing to activate and deactivate BWC through a single button on the front of the device. This timing is verbally directed by the on-scene supervisor and is strictly limited to the tactical portion of the operation. This significantly reduces the amount of potential exposure to personally identifiable information (PII) due to the limited time in which the BWC will actively capture and store audio and video. The BWCs will capture video footage and audio of individuals. Moreover, the system may capture additional PII through utterances and conversations during audio and video recording. The OIG will be using BWCs manufactured by Axon along with Axon systems and applications designed to support the use of Axon products. The specific Axon systems listed below are intended to be used by OI. These systems will collect PII though the capture of images and utterances of individuals, including investigative	

MODULE I – PRIVACY NEEDS ASSESSMENT

subjects, witnesses, other Agents and bystanders coming into contact with SAs deploying body cameras. This is in addition to the limited PII for user account information, which only includes the following information related to SAs: first and last name, email address, and badge number. However, utterances and conversations during audio and video recording could potentially capture PII. It is also possible to enter PII into the "note" fields within the Axon system due to the nature of open text capabilities.

Axon's cloud services hosted on US Axon FedCloud, which includes Axon Evidence, Axon Records, and other related offerings such as interactions between Axon Cloud Services and Axon Products. Axon's FedCloud has achieved FedRAMP Joint Authorization Board (JAB) Provisional Authority To Operate (P-ATO) at the High Impact Level.

Related Axon offerings that may be utilized by the OIG are described below:

- *Axon Evidence* is Axon's secure cloud-based Digital Evidence Management System (DEMS) hosted on US Axon FedCloud that OIG will use to store, manage, and track audio and video recordings, as well as manage internal users for access.
- *Axon View* is a mobile application for mobile devices (smartphones and tablets) that allows an agency user to wirelessly interact with a camera to view recorded videos, preview live video capture, and apply metadata to video files. It wirelessly connects with a camera to provide instant playback of unfolding events in the field. The user of the application sees what the camera sees.
- *Axon Capture* is a mobile application for mobile devices (smartphones) that allows an agency user to upload video, photo, and audio recordings captured on the users' smartphone directly to Axon Evidence. Rather than utilizing a separate recording device, such as a body-worn camera or in-vehicle camera, Axon Capture uses the recording capabilities of the smartphone. This application allows a smartphone to capture audio and video in lieu of the BWC, in exigent circumstances when the BWC is not available.
- *Axon Device Manager (ADM)* is a mobile application for mobile devices (smartphones and tablets) that allows the BWC Program Manager within OI to register, assign, and reassign Axon devices. In order to use the ADM application, the role of the user in Evidence.com must have a Device Administration permission, or Conducted Electrical Weapons (CEW) Administration permission, or both permissions set to 'Allowed' to use the ADM application. Though ADM is the preferred method for registering, assigning, and reassigning Axon devices, devices can also be registered, assigned, and reassigned directly in Evidence.com. This application is only used by System Administrators that have elevated privileges to provision hardware devices.

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address – FN, LN, Email Address, and Badge Number of agency users ☒ Other – Please Specify - BWC Audio and Video Footage relevant to the tactical portion of search and arrest warrants, individual encounters by SAs where the use of force may reasonably be anticipated, and interviews of subjects when deemed appropriate by the SA to capture the interaction or as requested by DOJ. Audio and video recordings could potentially contain images and utterances of PII, related to subjects of arrests and of others near the location where events take place. Open text fields in the Axon system could contain PII from data input against the text field's intended use.
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	PII exists on the system.

MODULE I – PRIVACY NEEDS ASSESSMENT

If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	Yes
2. Is the information in identifiable form?	Yes
3. Is the information about individual Members of the Public?	Yes
4. Is the information about DOE or contractor employees?	Yes ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY

What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?

- Executive Order 14074 (E.O. 14704) "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," dated May 25, 2022, requires that Federal Law Enforcement Agencies (FLEA) issue policies for use of Body Worn Cameras (BWC) during appropriate circumstances, to include during searches and arrests. E.O. 14704 further requires FLEA to develop BWC policy with requirements that are equivalent to or exceed the requirements in the US Department of Justice BWC policy.

- Public Law (PL) 95-452, the Inspector General Act of 1978, as amended [Title 5 United States Code (U.S.C.), Sections 401-424], sets forth authority and functions of the Inspector General and provides authorization to collect and maintain personal information to uncover fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement relating to DOE programs, operations, facilities, contracts, and information technology systems.

- In accordance with DOE O 221.2A, *Cooperation with the Office of Inspector General*, during the courses of audits, inspections, or investigations all DOE employees and contractors must:

    - Cooperate fully and promptly with requests from the OIG for information and data relating to DOE programs and operations;
    - Comply with requests for interviews and briefings and must provide affidavits or sworn statements, if so requested by an employee of the OIG so designated to take affidavits or sworn statements; and
    - Not impede or hinder other employees' cooperation with the OIG.

- Additionally, in accordance with DOE O221.2B, *Reporting Fraud Waste and Abuse to the Office of Inspector General*, employees and contractors must:

    - Report allegations and/or actual instances of fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement relating to DOE programs to the OIG; and,

MODULE II – PII SYSTEMS & PROJECTS	
	○ Supervisors must not impede, discourage, or prohibit employees from reporting such matters directly to the OIG.
2. CONSENT **What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?**	To effectuate the OIG's mission under the Inspector General Act of 1978, as amended, opportunities are not provided to individuals wishing to withhold or place limitations on investigatory information in the system. This information system is exempt from certain requirements under 10 CFR § 1008.12(a), which provides for an exemption for Investigative Files of the Inspector General (DOE-54). Moreover, 10 CFR § 1008.12(b)(2) provides a broad exemption for investigatory material compiled for law enforcement purposes. These exemptions enable the OIG to avoid notifying an individual at the individual's request of the existence of records in an investigative file pertaining to such individual or granting access to an investigative file in certain circumstances.
3. CONTRACTS **Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?**	Yes. The OIG's program is predicated on BWCs manufactured by Axon, which also controls system support for its products. However, Axon does not directly interact with data owned and controlled by its client. Axon personnel must request access from management through documented procedures in order to gain access to the US Axon FedCloud environment. Axon may use contractors to further design and maintain US Axon FedCloud. However, such contractors are required to enter into confidentiality agreements or Non-Disclosure Agreements. All Axon users are subject to Criminal Justice Information Services (CJIS) background checks and must agree to Acceptable Use and Rules of Behavior policies.

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The compromise of Axon's system could have a serious adverse effect on individuals based on the audio and video footage the system may contain relating to investigations of individuals and actions taken by law enforcement officers in execution of their duties. A compromise in this system could create significant harm and embarrassment for individuals including, but not related to, potentially significant reputational harm, professional harm, financial harm, embarrassment relating to the disclosure of behavior, identity harm, and damage to trust between individuals and the Federal Government, particularly for: 1. Arrestees seen or heard on videos before they are adjudged to be guilty of any crime and 2. Individuals whose images and utterances may be captured digitally who have no relation to the events precipitating the need for the cameras. The data in the system is relevant and necessary for the OIG to perform its statutory responsibilities. There will be no direct connections to other information systems, which will lower the risk of an indirect data breach via a different information system. Internally, the system will be strictly controlled, and authorized access to data is strictly limited to the administrator for the system and the individual capturing the data. Further restrictions exist that prevent the unauthorized or accidental disclosure of data in the system through internal controls. PII will be maintained in accordance with the Privacy Act and DOE requirements, and within applicable Federal records management requirements.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	PII is not used as an identifier for audio or video data captured by the system. Axon uses a unique identifier for audio and video captured based on time, date, and MD5 Hash values for authentication. MD5 Hashing is a function that authenticates the original data to ensure it has not been altered. The data captured is directly associated with a SA user account from which the data was created.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	• Investigative Files of the Inspector General (DOE-54) • Allegation-Based Inspection Files of the Office of Inspector General (DOE-83).
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	User account information will be input into the system by the OI system administrator. Data captured through audio and video recording will be through the use of an Axon BWC issued to a SA as part of their investigative authority.
9. Will the information system derive new or meta data about an individual from the information collected?	No.

MODULE II – PII SYSTEMS & PROJECTS

10. Are the data elements described in detail and documented?

Components	Does this Component Collect or Store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
Microsoft SQL Server Database Microsoft SQL Server Database	Yes	Text that may include PII if uploaded by customer Text that may include PII if uploaded by customer	Core system functionality Core system functionality	Entirely within authorization boundary Entirely within authorization boundary
Microsoft Azure Storage Microsoft Azure Storage	Yes	Video, voice recordings or other media files that a customer may upload into US Axon FedCloud Video, voice recordings or other media files that a customer may upload into US Axon FedCloud	Core system functionality Core system functionality	Entirely within authorization boundary Entirely within authorization boundary
Apache Cassandra Apache Cassandra	Yes	Text that may include PII if uploaded by customer Text that may include PII if uploaded by customer	Core system functionality Core system functionality	Entirely within authorization boundary Entirely within authorization boundary
Oracle MySQL Oracle MySQL	Yes	Text that may include PII if uploaded by customer Text that may include PII if uploaded by customer	Core system functionality Core system functionality	Entirely within authorization boundary Entirely within authorization boundary

DATA USE

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The identified PII of OIG employees (First and Last Name, Email Address, and Badge Number) will be used to associate user accounts for system use. Audio and video recordings will be used to create an auditable record of search and arrest warrants, protecting the OIG, arrestees, and individuals encountered during the tactical portion of a search warrant. These recordings may be used in subsequent criminal, civil, and administrative proceedings. Additionally, authorized recordings can be used internally for OIG training. These recordings will be redacted to protect PII where applicable and in accordance with federal law and OIG policy.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	Metadata is limited to date, time, and MD5 Hash value to identify the audio and video recording and is not associated with PII. Additionally, the system develops metadata based on user interaction with Axon Evidence for the purpose of evidence integrity and OIG internal auditing.
13. With what other agencies or entities will an individual's information be shared?	Data sharing is limited to joint investigative agencies and DOJ entities, such as United States Attorneys' Offices, with a need to know. BWC recordings will also be treated as potential evidence in a federal investigation subject to applicable federal laws, rules, and policies concerning chain of custody and any disclosure. Individual information regarding user accounts relative to Axon systems will not be shared outside OI.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	System user access and interaction reports.
15. What will be the use of these reports?	The BWC Program Manager will audit reports to ensure that only authorized users access the recordings and associated data for legitimate and authorized purposes.
16. Who will have access to these reports?	BWC Program Manager
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, as a result of geo metadata captured during recording.
18. What kinds of information are collected as a function of the monitoring of individuals?	Geolocation attached to a video during recording.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Geolocation metadata is captured and embedded as an encrypted attachment to recordings. Access to metadata is controlled by the BWC Program Manager in compliance with OI Policies. Strict hierarchy prevents the exposure of metadata to users through internal controls.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	User accounts will be controlled by the OI BWC Program Manager. Accounts no longer in use will be de-activated to prevent future access upon departure of the user from the agency or access to the system is no longer needed. Due to the nature of the audio and video captured, the data is maintained as original and will not be manipulated or updated due to its evidentiary value.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Consistent use is achieved through recurring user training and robust controls in Axon systems.
Records Management	
22. Identify the record(s).	Investigative Records
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Scheduled ▪ Investigative Records. (N1-434-00-1, Item 4)
24. Records Contact	Alexander Borman (Records Liaison Official) 202-586-1653 Alexander.borman@hq.doe.gov
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS	
25. What controls are in place to protect the data from unauthorized access, modification or use?	Axon uses a robust user hierarchy to control data access. Through these controls, the BWC Program Manager controls access to the system and grants user permissions based on the authorized level of access stated in OI policy. All original data is preserved to prevent unauthorized modification. Content redacted for privacy purposes does not affect the original content. A robust audit trail tracks all interactions with data and use in the system. Axon's FedCloud has achieved FedRAMP Joint Authorization Board (JAB) Provisional Authority To Operate (P-ATO) at the High Impact Level.
26. Who will have access to PII data?	• BWC Program Manager • Administrative users • Special Agents
27. How is access to PII data determined?	BWC Program Manager – Controls all access and requests for data in the system through approvals by the Assistant Inspector General for Investigations (AIGI) Administrative users may have access to data when approved by the AIGI and subsequently provided access by the BWC Program Manager. Special Agents will have access to the data created through their user account.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	N/A

MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?	BWC Program Manager

END OF MODULE I

SIGNATURE PAGE

	Signature	Date
System Owner	**Jeffrey Burnett** Jeffrey B. Burnett Digitally signed by Jeffrey B. Burnett Date: 2023.05.02 11:02:26 -04'00' **(Signature)**	
Local Privacy Act Officer	**Alexander Borman** Amy Sirignano for Alex Borman Digitally signed by Amy Sirignano for Alex Borman Date: 2023.05.02 11:58:13 -04'00' **(Signature)**	
Ken Hunt **Chief Privacy Officer**	**William K Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2023.05.02 10:53:00 -04'00' **(Signature)**	