Privacy Impact Assessment for the VA IT System called:

US Axon FedCloud – E

Veterans Affairs (VA) Central Office (VACO)

Office of Senior Security Officer (SSO), Operations 126

07/26/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Gina Siefert*	*Gina.siefert@va.gov*	*224-558-1584*
Information System Security Officer (ISSO)	*Bobbi Begay*	*Bobbi.begay@va.gov*	*720-788-4518*
Information System Owner	*Scottie Ross*	*Scottie.ross@va.gov*	*908-604-5278*

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

US Axon FedCloud - E is a tool that will be utilized by the VA police and police officers will have a body worn camera on their uniform and police vehicle mounted dash cameras that will have the capability of recording any triggered activity, including yelling, weapons pulling, shooting towards a police officer, and more. The cameras will begin the recording and will automatically upload the recording into the cloud, signal permitting. If no signal is found, at end of shift the cameras will be docked and the recordings will then be uploaded. The recordings will be uploaded into Axon's evidence system and will be retained as evidence in the SaaS tool.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

US Axon FedCloud – E, VACO Office of the Senior Security Officer, Operations 126

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

Axon Cloud Services (ACS) enables cloud-based workflows for digital evidence management, situational awareness, and records management to support the operational needs of agencies. US Axon FedCloud operates as an isolated region of Axon Cloud Services that is dedicated to the US Federal community. Axon Cloud Services offerings include Axon Evidence, Axon Respond, and Axon Records while also acting as the core control center over Axon devices and client applications. These devices and client applications include in-car camera systems (including the mobile data terminal), body-worn cameras, TASER devices, signal devices, Axon Interview Room, and Axon Upload XT; Axon Evidence, Axon Respond, and Axon Records modules. Axon Cloud Services (ACS) enables cloud-based workflows for digital evidence management, situational awareness, and records management to support the operational needs of agencies. Axon Evidence acts as a central repository for customers' digital evidence and a central management console for Axon products and devices. With expansive ingest, smooth playback, and intuitive search, Axon Evidence makes it simple to connect and manage growing stores of data—video, photos, documents and more—in a single, secure system. Axon Respond is a real-time operations platform which integrates real-time situational awareness and unified communications within a modern incident management solution. Gathering data from sensors in the field, agencies are empowered to know when events occur before it's voiced through traditional contact methods and rapidly coordinate responses with a unified communications platform. Axon Records harnesses the power of automation to save countless hours in the report writing, submission, and review process, helping agencies get more efficiency by breaking down data silos. With direct access to body-worn camera, in-car and citizen-captured video footage,

documents, images, and more, reports can be created faster. Critical evidence can be easily shared to remove the wall between digital evidence and reports.

C. Indicate the ownership or control of the IT system or project.
VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

There is no anticipated number of individuals whose information will be captured within the digital evidence solution. The typical individual will and can be veterans, employees, volunteers, and members of the general public. Veterans - the part of the population that is seen by the VA because they earned the benefits offered by the Government due to their Military service in a Military Branch, Employees - Personnel employed by the VA, Volunteers - personnel that volunteer to do things in conjunction with the VA, specifically help the VA deliver Benefits to a Veteran, and Members of the General Public - anyone that is outside of the categories of Veteran, Employee and Volunteer.

E. A general description of the information in the IT system and the purpose for collecting this information.

The data collected is for official law enforcement purposes, in accordance with President of the United States (POTUS) Executive Order 104740. Axon Cloud Services (ACS) enables cloud-based workflows for digital evidence management, situational awareness, and records management to support the operational needs of agencies. US Axon FedCloud operates as an isolated region of Axon Cloud Services that is dedicated to the US Federal community. Axon Cloud Services offerings include Axon Evidence, Axon Respond, and Axon Records while also acting as the core control center over Axon devices and client applications. These devices and client applications include in-car camera systems, body-worn cameras, TASER devices, Axon Interview Room, and Axon Upload XT.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

Axon Evidence is a multi-tenant environment where customers are logically separated. Customers are assigned unique FQDNs (Fully Qualified Domain Names) for their respective tenant or tenants e.g. a Federal customer will have a domain name that will look like ‘ https://agency.us.evidence.com’ (https://agency.us.evidence.xn--com-to0a/) where their name would be the ’agency’ subdomain. The application and databases services will capture all actions and ingest all data for their tenant to the appropriate database tables and storage containers. Storage containers hold the object data (evidence), and in the case of Azure Government, Azure Blob Storage is the storage used by Axon Evidence. Partner Agency sharing allows for agencies in the same region to share evidence and cases with each other through dedicated private connections. These relationships use a suite of APIs designed to identify and share evidence and cases between two separate Axon Evidence tenants. This allows agencies to work together and collaborate on cases more seamlessly. When an agency wants to share evidence, the agency will use the sharing services to send a sharing request to another agency. This request will traverse the web servers in the region, look up the DNS record (AWS Route53 for DNS services) of the recipient agency, and redirect the request back into the region to the appropriate agency’s API

endpoint. All requests and communications traverse the web servers and the WAF (web application firewall).

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The system used by the VA Police is located at a single location, Microsoft 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 US Axon FedCloud FedRAMP authorization. The FedRAMP Authorization process has a full set of criteria and requirements for how all PII, SPI and PHI are supposed to be handled and maintained to obtain the FedRAMP Authority to Operate. Those criteria's and requirement's must be maintained yearly to retain the authority to operate.
US Axon FedCloud operates in a posture where the actual system being utilized writes full backups to a backup site on a daily basis 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 the VA Police to do so and validate the integrity of the backup site and data to make sure the PII is fully in tack and correct.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records in these system of record are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program.

103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022

83VA07/87 FR 64146 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22900.pdf - A Police Badge and Training Records System VA – DTD 10/21/2022

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The addition of Audio and Video recordings constitutes a Significant Change for SORN 103VA07B/87 FR 64141 Police and Security Records. This SORN is in the process of being modified.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No Changes in the business process will result from this PIA completion.

K. Whether the completion of this PIA could potentially result in technology changes

No Changes in the technology changes will result from this PIA completion.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
• Place of birth
• Badge # / PIV ID

☐ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/Driver's License numbers*
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender

☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

• Duty Station
• VA email Address
• Religion
• Alien registration number
• Passport number
• Vehicle identifiers VIN
• Medical notes or other medical or health information
• Education records
• Certificates (Occupational, Education, Medical)
• User ID
• User passwords/codes

PII Mapping of Components (Servers/Database)

US Axon FedCloud – E consists of 0 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by US Axon FedCloud – E and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The information collected includes digital evidence such as audio, video, or still images that has been captured in the normal course of law enforcement emergency response duties. Personally Identifiable information (PII) may include video images of people, driver licenses, personal information verbally requested for the purposes of identifying individuals and/or arrests during a lawful contact. Information may also be obtained from publicly available sources, witnesses, concerned citizens, and any other sounds or images perceptible to the Body Worn Camera from its location on the wearer.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information is obtained from law enforcement camera systems, to include local recording systems, when the recording device is activated during law enforcement citizen interactions. Data recorded by the officer, or the camera is directly related to law enforcement activities and emergency response. Information may also be obtained from publicly available websites, witnesses, concerned citizens, and the general public providing images and recordings from their personally owned devices.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The Axon Records Module will have the ability to create reports.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is collected by law enforcement officers and their camera systems during face-to-face contact and/or interview, web sites, local recording systems, and information shared between system. Information can also be collected from interviews with individuals.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

No information is being collected on a form

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The majority of images captured through the digital evidence media are from VA law enforcement cameras in real-time. Recorded data collected that relates to individuals for an authorized purpose is verified by the law enforcement dispatch or communication center. For external sources, law

enforcement officials will verify the accuracy of data collected per policy and procedures defined by the organization. Supervisors will also review data for accuracy during the investigation process. All information will be reviewed for accuracy at least twice before final approval.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This system does not use a commercial aggerate to check for accuracy. All accuracy is checked by either the VA Police officer utilizing the data, a VA Police supervisor, a VA Police Compliance Officer, or VA Police Chief.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

VA Police Authority: 38 U.S. Code, Sections 901 & 902; VA Police Enforcement Authority: 38 Code of Federal Regulations 1.218; VA Police Procedures for Security and Law Enforcement: VA Handbook 0730; Executive Order 14074: Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Safety.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: PII and other highly delicate Sensitive Personal Information (SPI) could be captured on law enforcement camera systems when the recording device is activated, or additional information is added in support of an identified incident. Information may include video images of people, driver licenses, personal information verbally requested for the purposes of violation notices and/or arrests during law enforcement interactions. Data recorded is directly related to law enforcement activities and emergency response. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the minimum necessary information to identify the parties involved in an incident. However, due to the nature and purpose of the body worn camera (BWC) more information than needed may be collected. All users with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Every system user signs a national Rules of Behavior where they acknowledge they will follow VA privacy and information security rules. VA Handbook 5021 establishes and defines personnel sanctions for privacy and information security violations.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

.

Name, Social Security Number, Date of Birth, Financial Information, Tax Identification Number, Race/Ethnicity, Place of birth, Gender, Certificate/Driver's License numbers*, Badge # / PIV ID, Religion, Alien registration number, Passport number, Medical Record Number, Certificates (Occupational, Education, Medical), Education records, Integrated Control Number (ICN) – Used to clearly identify individuals and their records.

Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Personal Fax Number, VA email Address – Used to contact and communicate with individuals.

Emergency Contact Information (Name, Phone Number, etc. of a different individual), Mother's Maiden Name, Next of Kin – Used to contact or notify the appropriate individuals if the primary individual is not available.

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 purposes.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Searches of the system can be run to produce reports and track analytics. Types of reports include User Audit Trail Reports, User Summary Reports, Evidence Created Reports, User Device History Reports.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system creates records based on incidents that occur. Records can be retrieved based on individuals involved in the incident. The system does not create new information about an individual. Law Enforcement Officers can modify information to existing individual records.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Axon Data is protected in-transit with a minimum of TLS 1.2. Data is protected at rest utilizing AES 256-bit encryption.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

Axon encrypts all information at-rest within the system utilizing AES 256-bit encryption. Axon does not differentiate between content entered by customers.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

Law enforcement officers who have access to the system are required to hold a Public Trust security clearance. Through agency policy, on an annual basis each Officer is required to complete VA Privacy and Information Security Awareness and Rules of Behavior (TMS ID 10176). If employees have access to protected health information (PHI) they are required to take the Privacy and HIPAA Focused training (VA10203).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to US Axon FedCould -E and PII is given to authorized law enforcement officers within the VA after successful completion of the VA Police Academy (POST). US Axon FedCould -E and Cameras will be used by law enforcement officials, placed on the dashboard of law enforcement vehicles, or used by individual law enforcement officials on properties and locations within the jurisdiction of the VA.

Axon does store PII within the system. Axon is a custodian of SaaS Product, and Veteran's Affairs is the owner of Customer Content. Axon does not have visibility into the data stored within the system. As such, monitoring, auditing, and reporting are the responsibility of Veteran's Affairs.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

The Criteria, procedures, controls, and responsibilities regarding access is documented in the US Axon FedCould -E Standard Operating Procedure Manuals and all roles are taught by the Law Enforcement Training Center and the Facility VA Police Department.

2.4c Does access require manager approval?

Yes, any person requiring access to US Axon FedCloud -E must complete the Axon US Federal personnel security process and receive explicit approval from their manager and the system owner (or delegate). In addition, the VA Police Officer or Special Agent's Supervisor must submit the appropriate VA's application for that individual to receive their logical access to the US Axon FedCloud SaaS System.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes, all evidence and case files have an Audit Trail of the personnel who access the data and any actions executed against the data.

2.4e Who is responsible for assuring safeguards for the PII?

The US Axon FedCloud -E System Owner, Account managers, and authorized users are responsible for safeguarding PII. Each VA Police department is responsible for ensuring that all employees with access to a system of records are aware of the requirements of the Privacy Act and the Departmental Privacy Act regulations. Axon is responsible for the controls security detailed in the System Security Plan as well as the obligations defined in the Axon Cloud Services Privacy Policy.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Data with evidentiary relevance will be retained in the US Axon FedCloud -E. The following data elements may be retained within the system as per VA Police SOP:
Name
Social Security Number
Date of Birth
Mother's Maiden Name
Personal Mailing Address
Personal Phone Number(s)
Personal Fax Number
Personal Email Address
Emergency Contact Information (Name, Phone Number, etc. of a different individual)

Financial Information
Certificate/Driver's License numbers*
Vehicle License Plate Number
Internet Protocol (IP) Address Numbers
Medications
Medical Records
Race/Ethnicity
Tax Identification Number
Medical Record Number
Gender
Integrated Control Number (ICN)
Military History/Service Connection
Next of Kin
Place of birth
Badge # / PIV ID
Duty Station
VA email Address
Religion
Alien registration number
Passport number
Vehicle identifiers VIN
Medical notes or other medical or health information
Education records
Certificates (Occupational, Education, Medical)
User ID
User passwords/codes

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

National Archivist of the United States, Veterans Health Administration (VHA) Records Control Schedule (RCS)10–1- https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

Records will be maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States, Veterans Health Administration (VHA) Records

Control Schedule (RCS)10–1, 5252- Police Service, Physical Security and Protective Services Records.

Retention categories come out of the VHA RCS 10–1 are as follows:
5252.6 Unclaimed Personal Property Records, destroy when 3 years old or 3 years after the date title to the property vests in the Government, but longer retention is authorized if required for business use.
5252.9 Records of Routine Security Operations, destroy when 30 days old, but longer retention is authorized if required for business use.
5252.10 Accident and Incident Records, destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.
5252.13 Local Facility Identification and Card Access Records, destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.
5252.16 Canine (K-9) Service Records, destroy when superseded or obsolete, or 3 years after dog is released from service, whichever is sooner, but longer retention is authorized if required for business use.
5252.20 Information Security Violations Records, destroy 5 years after close of case or final action whichever occurs sooner, but longer retention is authorized if required for business use.
5252.23 Insider Threat Information, destroy when 25 years old, but longer retention is authorized if required for business use.
5252.25 Police and Security Records-VA/Police and Software Package, Cutoff at end of CY. Destroy 25 year(s) after cutoff.
5252.27 Video Surveillance Monitoring Records, Cutoff at midnight; destroy 30 days after cutoff or when no longer needed, whichever comes first.
5252.28 Electronic Video of Significant Incidents, Cutoff at the end of the significant or catastrophic event; destroy when 3 years old or when legal case, criminal case, or operational analysis is completed, whichever is later.
5252.33 Equipment Record File, Cutoff at end of FY. Destroy after 2 years. May be retained longer if needed.
5252.35 Reports (General/Miscellaneous), Cutoff at the end of CY. Destroy original after 1 year. Cutoff at the end CY. Destroy 3 years after cutoff.
5252.40 Personal Injury Files, Cutoff on termination of compensation or when deadline for filing a claim has passed; destroy 3 years after cutoff.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, Utilizes VHA RCS 10–1 schedule 5252- Police Service, Physical Security and Protective Services Records. National Archivist of the United States, Veterans Health Administration (VHA) Records Control Schedule (RCS)10–1- https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf & General Records Schedule - https://www.archives.gov/files/records-mgmt/grs/grs-trs34.pdf

3.3b Please indicate each records retention schedule, series, and disposition authority.

The below retention categories follow VHA RCS 10–1, Schedule 5252 Police Service, Physical Security and Protective Services Records and are as follows:

5252.6 Unclaimed Personal Property Records, DAA-GRS-2017-0006-0007;
5252.9 Records of Routine Security Operations, DAA-GRS-2017-0006-0012;
5252.10 Accident and Incident Records, DAA-GRS-2017-0006-0013;
5252.13 Local Facility Identification and Card Access Records, DAA-GRS-2017-0006-0018;
5252.16 Canine (K-9) Service Records, DAA-GRS-2017-0006-0021;
5252.20 Information Security Violations Records, DAA-GRS-2017-0006-0027;
5252.23 Insider Threat Information, DAA-GRS-2017-0006-0030;
5252.25 Police and Security Records-VA/Police and Software Package, DAA-0015-2016-0007-0002;
5252.27 Video Surveillance Monitoring Records, DAA-0015-2016-0007-0003;
5252.28 Electronic Video of Significant Incidents, DAA-0015-2016-0007-0004;
5252.33 Equipment Record File, II-NN-3270, item 16;
5252.35 Reports (General/Miscellaneous), 352-S84, II-NN-32706, II-NN-163-22, item 6;
5252.40 Personal Injury Files, N1-GRS-86-4, item 32.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1 Once the evidence has met its retention schedule, the evidence will be deleted and no longer accessible to any user in the US Axon FedCloud -E. Files are deleted from Azure Blob Storage 7 days after the deletion action. This file removal process leverages the Azure Government SaaS product Azure Blob Storage. File removal processes are inherited from Microsoft and validated as part of the FedRAMP High P-ATO process. Review of Microsoft Azure Government's POA&Ms shows no open issues for media sanitization (MP-6) which would cover this requirement."
https://my.axon.com/s/article/Categories-and-retention-policies?language=en_US

The Categories feature provides the ability to create policies, maintain them, and assign them to evidence. Categories include policy settings for evidence retention and restricted access for especially sensitive evidence.

Administrators or other users who are allowed the Category Administration permission can configure and delete categories.

Special and Pre-Configured Categories
Evidence.com includes two special categories:

- Uncategorized — Any evidence that is not assigned to another category is automatically assigned to the Uncategorized category. When you assign a category to evidence, it is automatically removed from the Uncategorized category.
- Pending Review

You cannot delete the Uncategorized or Pending Review category.

When your agency was created, we provided four additional categories that you can edit or delete as needed:

- Officer Injury
- Traffic Stop
- Training Demo
- Use of Force

Evidence Retention Policy
The evidence retention policy determines:

- Whether Evidence.com initiates automatic deletion of evidence assigned to the category.
- How long Evidence.com waits before initiating the deletion of evidence that is not included in a case. All evidence deletion dates, except for evidence submitted via Community Request, are calculated based on the *recorded on* date. Community Request evidence deletion dates are calculated based on the *uploaded on* date.

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion.

This policy applies to evidence only. Cases are never deleted automatically.

Evidence included in a case is exempt from deletion until it is removed from the case.

If evidence is in multiple categories, the longest retention time is used.

Evidence.com sends the following notification emails about evidence queued for deletion:

- Administrators receive a weekly email that summarizes upcoming agency-wide deletions.
- Users receive a weekly message regarding evidence that they uploaded.

For administrators, the Dashboard includes an Upcoming Evidence Deletions section that lists both user-initiated and system-initiated deletions.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No PII/live data is used for research, testing, or training purposes.

Axon does not use customer content which may include PII for testing, training, or research unless explicitly authorized by the customer.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the system may collect, store or share more information than necessary, or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

Mitigation: Controls are established in accordance with approved records retention schedules to ensure retention of images and video feeds does not exceed approved periods necessary for law enforcement purposes. VA restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (30 days) in accordance with approved records retention schedules for video recordings. The VA policy and records retention schedules dictates proper disposal of recordings at the end of the retention period and establishes specific policy and rules of behavior for the use of these audio/visual recording devices. Controls to mitigate these risks include: Access restrictions to authorized officials; Authorized use of information shared; Limits on uses and additional sharing; Retention periods and authorized destruction/ sanitization or return of information to the VA.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Inspector General (OIG)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Encrypted DVD/CD
Office of Accountability and Whistleblower Protection (OAWP)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	
Office of General Counsel (OGC)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	
Office of Operations, Security, Preparedness (OSP)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	
Veterans' Health Administration (VHA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	
Veterans Benefits Administration (VBA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	
Office of Information & Technology (OIT)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates	Encrypted DVD/CD

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
		• User ID • User passwords/codes • IP address	
National Cemetery Administration (NCA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address • Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Encrypted DVD/CD

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with sharing data within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: 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.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Local Police	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• IP address		
County Police	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD
State Police	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated)	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address		
Federal Bureau of Investigations (FBI)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address		
Central Intelligence Agency (CIA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD
Bureau of Alcohol, Tobacco, and Firearms (ATF)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address		
Drug Enforcement Agency (DEA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address		
Defense Health Agency (DHA)	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

Secret Service	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN) • Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD
Federal Prosecutors Office	Ongoing investigations	• Name • Date of birth or age • Place of birth • Badge # / PIV ID • Duty Station • VA email Address • Gender • Race, ethnicity, or citizenship • Religion • Social Security Number (full, last 4 digits or otherwise truncated) • Tax Identification Number (TIN)	Subpoena/Court Order SORN 103VA07B/87 FR 64141	Encrypted DVD/CD

		• Driver's license number • Alien registration number • Passport number • Mother's maiden name • Vehicle identifiers VIN • Vehicle License Plate • Personal mailing address• Personal e-mail address • Personal phone number • Medical records number • Medical notes or other medical or health information • Financial account information • Education records • Military status or other information • Certificates • User ID • User passwords/codes • IP address		

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of least privilege is strictly adhered by the system personnel. Only authorized personnel that have authenticated to the system are allowed access to the system and the information contained within the system. 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.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Some VA controlled areas may have signs posted that inform individuals of surveillance activities. Body worn cameras have indicator lights on when they are recording. In addition, uniformed officers, who the general public would recognize as having law enforcement authority, wear cameras visible to the public on their uniform or jacket. Given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of VA personnel or third parties. Body worn cameras do not collect PII/PII directly from individuals. Therefore, no notice is provided directly to the individual.
Generalized notice is provided by the publication of this notice of the SORN and the publication of this PIA. The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records in this system of record are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. 103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some VA controlled areas may have signs posted that inform individuals of surveillance activities but given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of VA personnel or third parties.
Generalized notice is provided by the publication of this notice of the SORN and the publication of this PIA. The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records in these system of record are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. 103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some VA controlled areas may have signs posted that inform individuals of surveillance activities but given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of VA personnel or third parties.
Generalized notice is provided by the publication of this notice of the SORN and the publication of this PIA. The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records in these system of record are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. 103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

No, 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. For use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some VA controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases notice may not be provided or consent obtained for audio or images captured during law enforcement operations or activities. Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements from a sexual assault victim, when a juvenile is involved, or as stipulated by policy.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

No, 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. For use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some VA controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases notice may not be provided or consent obtained for audio or images captured during law enforcement operations or activities. Exceptions to this policy and practice can occur when

individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements from a sexual assault victim, when a juvenile is involved, or as stipulated by policy.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Individuals may not be aware of publicly posted notices to include the SORN (103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022) and this PIA.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice. Individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some VA controlled areas may have signs posted that inform individuals of surveillance activities but given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of VA personnel or third parties.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

The Privacy Act governs the way VA collects, stores, provides access to, uses and discloses PII. Any individual requesting access to information will have to go through the VA's FOIA process through the Freedom of Information Act. Freedom of Information Act (va.gov)

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

Per SORN Police and Security Records—VA (103VA07B) and under Title 5 U.S.C., Section552a(j)(2), the head of any agency may exempt any system of records within the agency from certain provisions of the Privacy Act, if the agency or component that maintains the system performs as its principal function any activities pertaining to the enforcement of criminal laws. The function of the Police Service is to provide for the maintenance of law and order and the protection of persons and property on Department property. This system of records has been created, in major part, to support the law enforcement related activities assigned by the Department under the authority of Title 38 U.S.C. Section 901 to the Police Service. These activities constitute the principal function of this staff.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

Per SORN Police and Security Records- VA (103VA07B) Individuals seeking information on the existence and content of records in this system pertaining to them should write, call, or visit the VA facility where the records are maintained.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Per SORN Police and Security Records- VA (103VA07B) Individuals seeking to contest or amend records in this system pertaining to them should write, call or visit the VA facility where the records are maintained. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. A majority of records in this system are exempt from record access and amendment provisions of Title 5U.S.C., Sections 552a(j) and (k). To the extent that records in this system are not subject to exemption, individuals may request access and/or amendment. A determination as to whether an exemption applies shall be made at the time a request for access or contest is received.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking to contest or amend records in this system pertaining to them should write, call or visit the VA facility where the records are maintained. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it and the proposed amendment to the record. A majority of records in this system are exempt from record access and amendment provisions of Title 5U.S.C., Sections 552a(j) and (k). To the extent that records in this system are not subject to exemption, individuals may request access and/or amendment. A determination as to whether an exemption applies shall be made at the time a request for access or contest is received.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are provided with an avenue for redress. Per SORN Police and Security Records- VA (103VA07B)

Individuals seeking to contest or amend records in this system pertaining to them should write, call or visit the VA facility where the records are maintained. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. A majority of records in this system are exempt from record access and amendment provisions of Title 5 U.S.C., Sections 552a(j) and (k). To the extent that records in this system are not subject to exemption, individuals may request access and/or amendment. A determination as to whether an exemption applies shall be made at the time a request for access or contest is received.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*
Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals may not know how to seek redress or correction of their records as outlined in the Police and Security Records- VA (103VA07B) SORN. Individuals may become frustrated with results of their attempts.

Mitigation: Through the publication of this PIA and the SORN Police and Security Records- VA (103VA07B) the VA makes the public aware of the information that may be contained within this system. The SORN provides the public with notice on how to access information and how to redress/amend records in the system.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Access to US Axon FedCloud -E is restricted by a role-based and least privilege principles. Access to the evidence management system requires an active VA 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.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other agencies will have access to the VA Police US Axon FedCloud -E.
Axon does not provide infrastructure access to the SaaS to agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

VA Police

Role	**Functions Preformed**
FOIA	View and Redact video and reports shared with them.
Officers	View and share only their video evidence and reports.
Trainers	View and share only their video evidence and reports, assign cameras and docks.
Investigator	View and share only their video evidence and reports plus video redaction. Ability to create cases.
Supervisor	View and share their video evidence and reports plus any user they supervise. Creating cases and viewing audit logs.
VISN Chief/Local Chief	View and share their video evidence and reports, plus any user they supervise and can live stream video. Creating cases and viewing audit logs. Watching live stream body camera video.
Admin	View and share their video evidence and reports, plus any user they supervise and can live stream video. Creating cases and viewing audit logs. Add and edit users / permissions / roles / groups.

Axon

Role - Internal or External - Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) – Sensitivity Level - Authorized Privileges - Functions Performed

Axon Customer Support – Internal – P - Moderate - EDCA Customer Administration - Manage customer accounts including feature tiers, password resets, customer configurations.

Axon Engineering – Internal – P – High - Access to Infrastructure VPN and Azure Portal - Axon user administration for the infrastructure, install and configure software, OS updates, patches, and hotfixes, perform backups, develop code and applications, configure services and infrastructure, operate all system functions.

Axon Information Security Team – Internal – P – Moderate - Access to system logs via Infrastructure VPN, access to vulnerability scanning consoles - Reviews security events and logs, manages incident handling and response activities, schedules, and reviews vulnerability discovery scans.

JIRA VRR – Internal – NP – Low - Access to JIRA VRR instance - Review vulnerability tickets, execute JIRA ticketing workflows.

Microsoft Azure Government Hardware Support (GFS) – Internal – NLA - Moderate - Physical access to hardware that support underlying infrastructure services - Manage the physical security of the premises; Conduct patrols in and out of the Datacenter (DC) and Monitor all entry points; Perform escort services for certain non-cleared personnel who provide general services (dining, cleaning) into and out of the DC; Conduct routine monitoring and maintenance of network hardware; Perform incident management and break fix work using a variety of tools; Conduct routine monitoring and maintenance of the physical hardware in the datacenters; Perform break-fix work using a variety of tools; Provide escorting for non-cleared personnel providing IT work within the datacenter; Access to environment on demand from property owners. Capable to perform forensic investigations, logging IR& require mandatory security training &policy requirements; Operational ownership and maintenance of critical security tools such as scanners and log collection.

Microsoft Azure Government Software Support – Internal – NP - Moderate - Logical access to underlying infrastructure services - Debug and diagnose platform outages and faults for individual compute tenants and Microsoft Azure accounts; Analyze faults and drive critical fixes to platform /customer, drive technical improvements across support & Perform deployment/upgrades of platform components, software, and scheduled configuration changes in support of Microsoft Azure.

Axon Technology Services – Internal – NP - Moderate - EDCA Axon Administration - Adds, removes, and modifies Axon Personnel access to EDCA.

Axon Information Security Team – Internal – NP - Moderate - Access to system logs - Reviews, approves and enforces policy.

Axon Federal Customers – External - n/a - n/a - n/a - Customer usage of ACS.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or

employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

Non-Disclosure Agreement, VA Form 0752 shall be completed by all Contractor employees working on this contract and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete NDA prior to beginning work.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Axon provides security and privacy training to all persons with access to US Axon FedCloud, at minimum, annually.

VA offers privacy and security training, privacy and HIPAA training and specific role-based training depending on role assigned to the system. The Law Enforcement Center provides training on records management, as well as storing and collecting evidence.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? Yes

8.4a If Yes, provide:

1. *The Security Plan Status: Completed* as of 6/6/2023.
2. *The System Security Plan Status Date:* 6/8/2023
3. *The Authorization Status:* Conditional Authority to Operate.
4. *The Authorization Date:* 7/15/2023
5. *The Authorization Termination Date:* 1/11/2024
6. *The Risk Review Completion Date:* 7/1/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

Yes, the system uses Cloud Technology, US Axon FedCloud is a FedRAMP Authorized SaaS hosted on Azure Gov Cloud, US Axon FedCloud is software as a service (SaaS). US Axon FedCloud maintains a FedRAMP High Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board (JAB).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

The VA Police Cameras and Evidence Cloud Storage: Contract # 36C10X22D0024 is currently in place as awarded by the Strategic Acquisition Center – Fredericksburg.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

Axon collects non-content data. Non-Content Data includes data, configuration, and usage information about customer's Axon Cloud Services tenant, Axon Devices, Axon Client

Applications, and users that is transmitted or generated when using Axon Products. Non-Content Data includes the following:

Customer Entity And User Data

Customer Entity and User Data includes personal and non-personal data regarding Customer's Axon Cloud Services tenant configuration and users. Axon uses Customer Entity and User Data to: (1) provide Axon Cloud Services, including, without limitation, user authentication and authorization functionality; (2) improve the quality of Axon Products or provide enhanced functionality and features; (3) contact Customer to provide information about its account, tenant, subscriptions, billing, and updates to Axon Cloud Services, including, without limitation, information about new features, security and other technical issues; and (4) market our products or services to Customer via email, by sending promotional communication including targeted advertisements, or presenting a Customer with relevant offers.

Customer cannot unsubscribe from non-promotional communications but may unsubscribe from promotional communications at any time.

Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data includes data regarding Customers' interactions with Axon Cloud Services and Axon Client Applications. Axon uses Customer Entity and User Service Interaction Data to improve the quality of Axon Products and provide enhanced functionality and features.

Service Operations and Security Data

Axon uses Service Operations and Security Data to provide service operations and monitoring.

Account Data

Axon uses Account Data to provide Axon Cloud Services, manage Customer's accounts, market to, and communicate with Customer. Customer may unsubscribe from promotional communications at any time.

Support Data

Axon uses Support Data to resolve Customer’s support incident, and to operate, improve, and personalize Axon Products. If Customer shares Customer Content to Axon in a support scenario, the Customer Content will be treated as Support Data but will only be used for resolving support incidents.

Axon may provide support through phone, email, or online chat. With Customer's permission, Axon may use Guest Access ("GA") to temporarily navigate Customer's Axon Cloud Service's tenant to view data in order to resolve a support incident. Phone conversations, online chat sessions, or GA sessions with Axon support professionals may be recorded and/or monitored.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Responsibilities are defined within the Axon Master Services and Purchasing Agreement and Axon Cloud Services Terms of Use Appendix. Roles are further defined in the Axon Cloud Services Privacy Policy (https://www.axon.com/legal/cloud-services-privacy-policy). Axon's Role Axon is a Data Processor of Customer Content. Customer controls and owns all right, title, and interest in and to Customer Content and Axon obtains no rights to the Customer Content. Customer is solely responsible for the uploading, sharing, withdrawal, management and deletion of Customer Content. Customer grants Axon limited access to Customer Content solely to provide and support Axon Cloud Services to and for Customer and Customer's end-users. Customer represents and warrants to Axon that: (1) Customer owns Customer Content; (2) and Customer Content, and Customer's end-users' use of Customer Content and Axon Cloud Services, does not violate this Policy or applicable data protection laws and regulations. Axon may also collect, control, and process Non-Content Data. Axon is a Data Controller for Non-Content Data. Axon collects, controls, and processes Non-Content Data to provide Axon Cloud Services and to support the overall delivery of Axon Products including business, operational, and security purposes. With Non-Content Data, Axon may analyze and report anonymized and aggregated data to communicate with external and internal stakeholders. In regard to Customer Entity & User Data, Axon is a Data Controller and Customer is an independent Data Controller, not a joint Data Controller with Customer.

Veteran's Affairs Role
Customer Content

Customer can access Customer's tenant to manage Customer Content.

Non-Content Data

Within the scope of Axon's authorization to do so, and in accordance with Axon's commitment under the Privacy Shield, Axon will work with Customers to provide access to Personal Data about Customer that Axon or Sub-processors holds. Axon will also take reasonable steps to enable Customers to correct, amend, or delete Personal Data that is demonstrated to be inaccurate.

If at any time after registering an account on Axon Cloud Services you desire to update Personal Data you have shared with us, change your mind about sharing Personal Data with us, desire to

cancel your Customer account, or request that Axon no longer use provided Personal Data to provide you services, please contact us at privacy@axon.com. We will retain and use Personal Data for as long as needed to provide you services, comply with our legal obligations, resolve disputes, and enforce our agreements.

Certain data processing is determined by Customer based on Axon Product usage, Customer network or device configuration, and administrative settings made available with Axon Cloud Services or Axon Client Applications:

Axon Body 3 WiFi Positioning

Axon Body 3 cameras offer customers a feature to enhance location services where GPS/GNSS signals may not be available, for instance within buildings or underground. Customer administrators can manage their choice to use this service within the administrative features of Axon Cloud Services. When WiFi Positioning is enabled, Non-Content and Personal Data including location, device and network information data will be sent to Skyhook Holdings, Inc (Skyhook) to facilitate the WiFi Positioning functionality. Skyhook will act as both a data sub-processor (as reflected in this policy) and as a data controller. Skyhook becomes a data sub-processor for Axon when Skyhook processes data from Axon Body 3 devices to determine a location. Skyhook acts a data controller when it collects data sent from Axon Body 3 cameras to maintain their services and to develop new products, services or datasets. Data controlled by Skyhook is outside the scope of the Axon Cloud Services Privacy Policy and is subject to the Skyhook Services Privacy Policy.

Client Push Notifications

Axon Products leverage push notification services made available by mobile operating system providers (i.e. Google's Cloud Messaging and Apple's Push Notification Service to deliver functional notifications to client applications. Push notification services can be managed by leveraging notification settings made available in both mobile applications and the mobile operating system.

User Analytics

Customers can opt-out of user analytics tracking on Axon Cloud Services by disabling cookies or preventing Customer's browser or device from accepting new cookies. To prevent data from being collected by Mixpanel, network or device access to *.mixpanel.com should be blocked

Service Support

Mobile client application crash analytics are used provide Axon personnel insight to crashes when using Axon client applications. To opt out of crash reporting, network or device access to *.crashlytics.com should be blocked.

Geolocation Services

Geolocation services are critical to proper user functionality of many of Axon products. However, customers can chose to opt out of mapping and geolocation functionality by blocking network or device access to *.mapbox.com and *.arcgisonline.com

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

US Axon FedCloud provides the assisted services Auto-transcribe and Redaction Studio. These services assist in management of data, but the output should always be validated. Redactions should be validated to ensure sensitive information is obfuscated and Transcriptions should be validated for and updated for accuracy.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2023.08.07 08:21:13 -05'00'

Privacy Officer, Gina Siefert

BOBBI DEE BEGAY Digitally signed by BOBBI DEE BEGAY
Date: 2023.08.07 12:43:41 -06'00'

Information Systems Security Officer, Bobbi Begay

SCOTTIE ROSS Digitally signed by SCOTTIE ROSS
Date: 2023.08.08 18:53:47 -04'00'

Information Systems Owner, Scottie Ross

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms).

The authority to maintain these records is Title 38, United States Code (U.S.C.), Section 501 and 901–905. The records in this system of record are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. 103VA07B/87 FR 64141 - https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf - Police and Security Records-VA - 10/21/2022

Freedom of Information Act (va.gov)

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Scheduler: Transmittal 34

https://www.archives.gov/files/records-mgmt/grs/grs-trs34.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Handbook 1605.04: Notice of Privacy Practices