US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/22/2025

OPDIV:

NIH

Name:

ORS Investigations Audio Visual

PIA Unique Identifier:

P-7495233-391689

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

This validation is intended to refresh content and update the status of Investigations-Audio Visual (IAV).

Describe the purpose of the system.

The primary purpose of Investigations-Audio Visual (IAV) is for the recording of law enforcement interviews. The IAV increases evidence strength and confidence during an NIH Division of Police (DP) investigation by utilizing CaseCracker Onyx (Windows client app launches right from the user's PC) application and recording suite.

IAV is maintained in an isolated and silo-ed (of a system, process department) environment that has no access or connection to NIH Enterprise Network Services (ENS) (allows for a shortened version of your wallet address), Federal Acquisition Computer Network (FACnet) nor Internet.

Describe the type of information the system will collect, maintain (store), or share.

The DP investigator will use the IAV system to record criminal investigation interviews that includes Personally Identifiable Information (PII). This is contingent upon the subject of the interview and/or any situation(s) discussed during the interview. PII data will be incorporated into the video interview recordings and is mandatory for law enforcement purposes and identification purposes. The IAV recording will collect and maintain (store): name, driver's license, email, mailing address, social security number (SSN), phone number, vehicle identification, date of birth, mother's maiden name, employment status, passport number, photographic identifiers as well as audio visual recordings of individuals who have been arrested.

Although the system collects a video, it does not use it to identify anyone through biometric markers, such as voices or facial recognition. These recordings can also be related to internal affairs.

Due to security concerns of evidence tampering, the IAV system operates in an isolated and silo-ed environment where access is limited and controlled. IAV has no connection to a network or the internet. These recordings are maintained and secured within the physically controlled IAV environment and secured room limited to the System Owner and Technical Administrator. Users must go through several layers of access-controlled entry points to get to this location. The recorded data can only be accessible to users that are approved to access IAV by physical and system environments. For situations requiring remote interviews, an IAV satellite laptop will be utilized. This is stored in the IAV room and used as needed. The laptop operates independently and does not have any connection to the primary IAV system, network or the internet.

Users login into the system by using a shared username and password.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The primary purpose of the Investigations-Audio Visual (IAV) is for the recording of law enforcement interviews. The IAV increases evidence strength and confidence during a NIH Division of Police (DP) investigation by utilizing CaseCracker Onyx (Windows client app launches right from the user's PC) application and recording suite.

IAV is maintained in an isolated and silo-ed (of a system, process department) environment that has no access or connection to NIH Enterprise Network Services (ENS) (allows for a shortened version of your wallet address), Federal Acquisition Computer Network (FACnet) nor Internet.

The DP investigator will use the IAV system to record criminal investigation interviews that may include Personally Identifiable Information (PII). This is contingent upon the subject of the interview and/or any situation(s) discussed during the interview. PII data will be incorporated into the video interview recordings and is mandatory for law enforcement purposes and identification purposes. The IAV recording will collect and maintain (store): name, driver's license, email, mailing address, social security number (SSN), phone number, vehicle identification, date of birth, employment status, passport number, photographic identifiers as well as audio visual recordings of individuals who have been arrested.

Although the system collects a video, it does not use it to identify anyone through biometric markers, such as voices or facial recognition. These recordings can also be related to internal affairs.

Due to security concerns of evidence tampering, the IAV system operates in an isolated and silo-ed environment where access is limited and controlled. IAV has no connection to a network or the internet. These recordings are maintained and secured within the physically controlled IAV environment and secured room limited to the System Owner and Technical Administrator. Users

must go through several layers of access-controlled entry points to get to this location. The recorded data can only be accessible to users that are approved to access IAV by physical and system environments.

An IAV satellite laptop will be utilized in case of failure of the primary system. This is stored in the IAV room and used as needed. The laptop operates independently and does not have any connection to the primary IAV system, network or the internet.

Users login into the system by using a shared username and password.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Employment Status
Passport Number
username and password
audio visual recordings

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

The primary purpose of the collected PII is for accurate identification and evidence in criminal case investigations. In some cases, these recordings are taken to a formal court of law.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

40 U.S.C. § 1315 Law enforcement authority of Secretary of Homeland Security for protection of public property; General Administrative Delegation of Authority Number 08, Control of Violations of Law at Certain NIH Facilities (September 1, 2020).

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0224, NIH Division of Police Records.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Other

Government Sources

Within DPD

State/Local/Tribal

Non-Governmental Sources

Public

Other

Identify the OMB information collection approval number and expiration date

N/A. The Paperwork Reduction Act exempts federal agencies from requiring clearance for information collected during criminal investigations or prosecutions.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) are not applicable. Collected evidence is not readily shared with other agencies/courts unless the NIH receives a subpoena for potential evidence in their criminal investigation and case. The subpoena will be received by the DP Chief and if required, the NIH General Counsel before release of the interview. Also all transfer records are maintained and documented as a release of evidence within the Commercial Dispatch and Reporting System (CODY) system. The CODY system has its own Privacy Impact Assessment (PIA).

Describe the procedures for accounting for disclosures.

Also all transfer records are maintained and documented as a release of evidence within the CODY system.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Individuals are notified verbally that information is being collected by the IAV representative and/or as part of the evidence-informed decision making (EIDM) application. The recorded interview incorporates notification and acceptance process for the individual to validate/document their identification with PII information.

Also all transfer records are maintained and documented as a release of evidence within the CODY system. CODY maintains its own PIA, including all legal authorities documented.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no ability to opt-out. PII information is used to validate the person being interviewed in the evidence-informed decision making (EIDM) application during a criminal investigation and is incorporated into the video recording. If there are any amendments to the original video, the requestor has the opportunity to request another interview to amend their responses, however the original video cannot be tampered with or changed as this is evidence that's part of a legal and criminal investigation.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

This system of records is exempt from notification procedures to the extent permitted by 5 U.S.C. 552(j)(2) or (k)(2). However, consideration will be given to any notification request addressed to the System Manager.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals concerned that their PII has been inappropriately obtained, used, or disclosed, or is inaccurate, can contact the NIH Department of Police by email at rowlandc@ors.od.nih.gov.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic audits are conducted to ensure the data's integrity, availability, accuracy, and relevancy. The system produces reports for review by the system administrator.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

All systems users are vetted and must receive prior approval from an authorized DP supervisor before being added as a system user.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations conform to role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.

gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

The NIH DP personnel receive on-the-job-training to use the IAV System by in house certified trainers.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are retained and disposed of under the authority of the following NIH Records Retention Schedules.

NIH GRS 08-204, Information Access and Protection Records
Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.
Disposition Authority Agency (DAA)-GRS-2019-0001-0002

NIH GRS 08-228 Controlled Unclassified Information (CUI) Information sharing agreements.
Destroy 7 years after canceled or superseded, but longer retention is authorized if required for business use.
DAA-GRS-2019-0001-0006

NIH GRS 09-413 Operations and Facilities Management. 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.
DAA-GRS-2021-0001-0004

NIH GRS 09-422, Operations and Facilities Management. Personnel security investigative reports.
Personnel suitability and eligibility investigative reports.
Destroy in accordance with the investigating agency instruction.
DAA-GRS-2017-0006-0022

NIH GRS 09-423, Operations and Facilities Management.
Destroy in accordance with delegated authority agreement or memorandum of understanding.
DAA-GRS-2017-0006-0023

NIH GRS 09-427 Security Management Records
Destroy 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.
DAA-GRS-2017-0006-0027

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: All technical personnel who access information technology (IT) systems which contain protected information have met background investigation criteria for Public Trust positions.

Physical Controls: The IT hardware used to host protected information is located in a secured room within the DP facilities. This room is only open to authorized personnel whose access is monitored by locking doors with badge readers, which logs the access event. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public and NIH networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored locally to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel and managed by the system Administrator.

The users/administrator will require an independently established username/password to access the system. These system and application login accounts are managed by the System Owner and Technical Administrator to control and limit user access.

IAV recorded data will be stored within the IAV system that is in the secured access-controlled room. IAV recordings will only be released upon the following conditions:

Criminal evidence requests - This will require approvals from the DP Chief and must be documented and recorded within the CODY system. Evidence recording will be provided by a password protected and encrypted Universal Serial Bus (USB) drive that is approved by NIH security. The password management will follow NIH security protocols.
Data backups - Interview recordings will be backed up onto approved USB drives and maintained by the System Owner within a combination controlled safe located in an alternate access-controlled location. These NIH approved USB drives will be password protected and encrypted. The System Owner and Technical Administrator will maintain, manage, and secure the backup USBs. Please note that there is a written approval by the ORS & ORF Chief Information System Security Officer for the use of these encrypted USBs.

IAV satellite laptop - The laptop is kept within the secured IAV room and used remotely as required. The temporary recorded interviews are immediately transferred to the main IAV server via a recordable compact disc/digital video recorder (CD or DVD). Once stored, the recorded media is shredded and destroyed according to NIH media protection requirements and the interview file is deleted from the laptop.