U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

PRIVACY IMPACT ASSESSMENT

OSHA INJURY TRACKING APPLICATION (ITA)

VERSION 1.1

JUNE 12, 2023

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/17/22	ITA PIA_Nov172022/1.0	T.Colson	Initial Draft
6/12/2023	ITA PIA_06122023/1.1	T. Colson	Updated to include SOL changes
6/29/2023	ITA PIA_06292023/1.1	D. Schmidt	Updated to include csv issues

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
6/2/2023	ITA PIA_06122023/1.1	SOL – Robert Aldrich and Allison Kramer
6/28/2023	ITA PIA_06292023/1.1	SOL – Robert Aldrich and Louise Betts

TABLE OF CONTENTS

1.1 OVERVIEW

OSHA's regulation at 29 CFR 1904 requires employers with more than 10 employees in most industries to keep records of occupational injuries and illnesses at their establishments. Employers covered by the regulation must use three forms, or their equivalent, to record employee injuries and illnesses:

- OSHA Form 300, the Log of Work-Related Injuries and Illnesses. This form includes information about the employee's name, job title, date of the injury or illness, where the injury or illness occurred, description of the injury or illness (*e.g.*, body part affected), and the outcome of the injury or illness (*e.g.*, death, days away from work, job transfer or restriction).
- OSHA Form 301, the Injury and Illness Incident Report. This form includes the employee's name and address, date of birth, date hired, and gender and the name and address of the health care professional that treated the employee, as well as more detailed information about where and how the injury or illness occurred.
- OSHA Form 300A, the Annual Summary of Work-Related Injuries and Illnesses. This form includes general information about an employer's workplace, such as the average number of employees and total number of hours worked by all employees during the calendar year. It does not contain information about individual employees. Employers are required to prepare this form at the end of each year and post the form in a visible location in the workplace from February 1 to April 30 of the year following the year covered by the form.

The OSHA Injury Tracking Application (ITA) is the system that provides employers the means to meet the annual electronic reporting requirements in 29 CFR 1904.41. Specifically, employers that meet certain establishment size and industry criteria are required to electronically submit certain information from their injury and illness recordkeeping forms to OSHA once a year. Employers create an account in the ITA and on an annual basis login to the system, enter the required data, certify its accuracy, and submit the data. OSHA intends to post some of the collected data on a public website after identifying and redacting information that could reasonably be expected to identify individuals directly, such as individuals' names and contact information.

DOL describes Personal Identifiable Information (PII) as:

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

The OSHA Injury Tracking Application is a multi-tier containerized application which includes a front-end tier using React.js, a middle-tier using Drupal (utilizing Drupal 9, PHP7 and Docker container), an Azure queue service for storing CSV submissions, and a backend-tier using Java (utilizing Spring Framework).

- React is used for User Experience to display the User Interface (UI) elements, defined in a JSON object retrieved from Drupal.
- Drupal is used to authenticate user actions (various API calls) and manage Form and Form Question content. User account information is stored in the ITA Drupal database.
- Azure Queue Service acts as interim database to save CSV file submissions. These files are retrieved and validated by Java backend of the application.
- Java backend is used to retrieve and store data in MYSQL database. Also, the validation for the establishment and 300A, 300 and 301 data is performed in the JAVA backend.
- ITA 300A, 300, 301 and establishment data is stored separately from Drupal content in a MySQL database.

1.2 CHARACTERIZATION OF THE INFORMATION

ITA collects and maintains occupational injury and illness information that employers are already required to keep under OSHA's recordkeeping regulation at 29 CFR 1904. Covered employers must electronically submit the following information to OSHA on an annual basis.

- Business Entity
  - EIN (not required)
  - Company Name
  - Company Address
  - NAICS
  - Size (number of company employees)
  - Government (Yes or No)
  - Form 300A Data
  - Form 300 Data
  - Form 301 Data

- From whom is information to be collected?

Establishments with 20 to 249 employees in certain industries are required to electronically submit information from their OSHA Form 300A annual summary to OSHA once a year. See, 29 CFR 1904.41(a)(1)(i).

All establishments (regardless of industry) with 250 or more employees that are also required to keep records under OSHA's injury and illness recordkeeping regulation are required to electronically submit information from their Form 300A to OSHA on an annual basis. See, 29 CFR 1904.41(a)(1)(ii).

Establishments with 100 or more employees in certain designated industries are required to electronically submit information from their OSHA Forms 300 and 301 to OSHA once a year. See, 29 CFR 1904.41(a)(2).

Data is collected on an annual basis from covered establishments on the number and type of occupational injuries, illnesses, and deaths that occurred during the previous calendar year.

- For the OSHA Form 300A (Annual Summary of Work-Related Injuries and Illnesses), covered establishments must electronically submit the following information to OSHA once a year:
  - Annual average number of Employees
  - Total hours worked by All Employees
- Number of Cases (Total Number)
  - Deaths
  - Cases with days away from work
  - Cases with job transfer or restriction
  - Other recordable cases
- Number of Days
  - Days away from work
  - Days of job transfer or restriction
- Injury and Illness Types (Total number of)
  - Injuries
  - Skin Disorders
  - Respiratory conditions
  - Poisonings
  - Hearing loss
  - All other illnesses

For the OSHA Form 300 (Log of Work-Related Injuries and Illnesses), covered establishments must electronically submit the following information about each recorded injury and illness:

- Job title
- Date of injury or onset of illness
- Where the event occurred
- Description of the injury or illness (e.g., parts of body affected, and object/substance that directly injured or made the employee ill.
- Whether the injury or illness resulted in death, days away from work, job transfer or restriction, or other recordable cases (e.g., medical treatment beyond first aid).

Note: Covered establishments are not required to electronically submit to OSHA information in Column B (employee name) from the OSHA Form 300. See. 29 CFR 1904.41(b)(9).

For the OSHA Form 301 (Injury and Illness Incident Report), covered establishments must submit the following information about each recorded injury and illness:

- Date of birth (field 3)
- Date hired (field 4)
- Gender (field 5)
- Was employee treated in an emergency room? (field 8)
- Was employee hospitalized overnight as an inpatient? (field9)

- Case number from the Log (field 10)
- Date of injury or illness (field 11)
- Time employee began work (field 12)
- Time of event (field 13)
- What was the employee doing just before the injury or illness (field 14)
- What happened? Tell us how the injury occurred (field 15)
- What was the injury or illness? (field 16)
- What object or substance directly injured the employee? (field 17)

Note: Covered establishments are not required to electronically submit to OSHA information from the OSHA Form 301 about employee name (field 1), employee address (field 2), name of physician or healthcare professional (field 6), and facility name and address if treatment was given away from the worksite (field 7).

- Why is the Information being collected?
  The information is being collected to help OSHA track the number and type of occupational injuries, illnesses, and deaths in the United States. OSHA will use the collected data to identify workplace hazards and target specific establishments for its enforcement inspection and compliance assistance programs. Some of the collected data will be made available to the public to increase knowledge about workplace hazards. The ultimate goal of the submission requirement is to increase knowledge of workplace hazards, improve worker safety and health, and reduce the number of occupational injuries and illnesses.

- What is the PII being collected, used, disseminated, or maintained?
  - As noted above, direct identifiers, such as employee name and address are not being collected by OSHA. In addition, the OSHA recordkeeping forms include warnings to employers not to include identifiable information in their entries. OSHA also includes reminders on the ITA website to establishments not to electronically submit information that could reasonably be used to identify individuals directly. Since information entered on the recordkeeping forms about names and addresses are not being submitted to OSHA by covered establishments, the only collection of PII will be inadvertent (e.g., PII may be included in narrative descriptions of injuries and illnesses).

- How is the PII collected?
  - Covered establishments are required to submit information about an injured or ill employee's job title, date hired, and gender that, in some limited circumstances, could be used to identify individual employees. Covered establishments are also required to submit information about an injured or ill employee's date of birth, but the ITA automatically converts this information to "age." In addition, PII could potentially be inadvertently included in the submissions by covered establishments in the narrative fields from the OSHA Form 301.

Note: In order to enhance privacy, certain information from the OSHA Form 301, such as employee age, date hired, gender, whether the employee was treated in an emergency room, and whether the employee was hospitalized overnight as an inpatient, will be collected and retained by OSHA, but will not be made publicly available.

- How will the information collected from individuals or derived from the system be checked for accuracy?
  - The covered establishments that electronically submit the information to OSHA are responsible for reviewing and certifying the accuracy of the data they submit.

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?
  - The Occupational Safety and Health Act of 1970, (OSH Act) authorizes OSHA to issue requirements for the recording and reporting of occupational injuries and illnesses. The electronic submission of injury and illness data by certain establishments is required by 29 CFR 1904.41.

- Privacy Impact Analysis
  Privacy risks are low because PII is not generally entered into the system. PII may be inadvertently submitted by covered establishments. However, OSHA will use de-identification technology to identify and redact information from the system that could reasonably be used to identify individuals directly. OSHA does not intend to post any PII collected from the electronic submission on its public website.

1.3 DESCRIBE THE USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used. This section is informational only.

- Describe all the uses of the PII
  - The date of birth will be used to calculate the age of the injured or ill worker. This data will not be associated with any individual personal identifiers and will not be made publicly available. The system will collect information about date of birth, but will automatically convert the information to age. Note that the DOB will not be retained in the ITA system. Information about the age of an injured or ill employee is important in determining whether younger or older employees are more susceptible to certain types of injuries and illnesses. Likewise, although not published on the public website, other collected information, such as date hired or gender, is important to OSHA in analyzing trends about specific injuries and illnesses to certain workers.

- What types of tools are used to analyze data and what type of data may be produced?
  - Individual case data (the raw data) will be collected and published after identifiable information is identified and redacted.

- OSHA also intends to classify and publish the data using the BLS OIICS coding system for analysis by interested parties. The agency will use auto coding technology.

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
  - OSHA does not intend to aggregate the data collected.

- If the system uses commercial or publicly available data, please explain why and how it is used.
  - The system does not use publicly available data.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?

No. The Privacy Act only applies to records that are located in a "system of records." As defined in the Privacy Act, a system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" (*see* 5 U.S.C. 552a(a)(5)). Because OSHA injury and illness records are retrieved neither by the name of an individual, nor by some other personal identifier, the Privacy Act does not apply to OSHA injury and illness recordkeeping records. As a result, the Privacy Act does not prevent OSHA from posting recordkeeping data on a publicly accessible website.

- Privacy Impact Analysis
  - ITA adheres to federally mandated and DOL policy and procedures for access control and authentication and authorization that are built into the applications.

1.4 RETENTION

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

- What is the retention period for the data in the system?
  - Indefinitely. Information retained until decommissioning of the system/applications

- Is a retention period established to minimize privacy risk?
  - No. Other safeguards have been built into the collection and publication system to protect private information.

- Has the retention schedule been approved by the National Archives and Records Administration (NARA)?
  - No. OSHA is currently in the process of scheduling the data with NARA.

- Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?
  - Covered establishments are required to submit information about an injured or ill employee's date of birth (DOB). However, the system will automatically convert DOB to age and delete all specific information about DOB from the ITA database. Users that submit their data by csv file include the DOB in the csv file. As the data are successfully uploaded into the ITA, the conversion of DOB to age will occur immediately and only the age will be retained within the ITA database. The originally submitted csv files, which include DOB, will be temporarily stored in an encrypted cloud storage space, managed by the Department of Labor's IT system. OSHA has a business need to retain the csv files on a temporary basis. Specifically, when a csv file fails to load due to edit check failures, the OSHA Help Desk needs to access the files to resolve the problem(s). The csv files will be deleted from the DOL IT system on a regular basis.
  - OSHA will use de-identification technology to identify and redact information in the ITA system that could reasonably be expected to identify individuals directly.

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?
  - Yes

- How is it determined that PII is no longer required?
  - Business functionality determines when PII is no longer required.

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

- Our efforts to de-identify PII will be outside the system (we intend to use commercial off-the-shelf software).
- For text-based data, OSHA plans to use automated de-identification technology, supplemented with some manual review of the data, to identify and remove information that could reasonably be expected to identify individuals directly from the fields the agency intends to publish; the agency will not publish text-based data until such information, if any, has been identified and removed.

- Privacy Impact Analysis
  - There is a low level of risk with misuse of private data, primarily due to inadvertent use of protocol sharing of the data that does not conform to the standards.

1.5 INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- With which internal organization(s) is the PII shared, what information is shared, and for what purpose?
  - The data collected, including the fields with potential PII, will be shared with the Bureau of Labor Statistics. BLS and OSHA both collect the same data from an overlap of respondents. Sharing data with the BLS can potentially reduce the reporting burden of the overlap respondents.

- How is the PII transmitted or disclosed?
  - BLS can access the data through an Application Program Interface (API).

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?
  - No. There will be a consistent sharing indefinitely of this ITA data with BLS.

- Privacy Impact Analysis
  - The risk to privacy from internal sharing is low.

1.6 EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state and local government, and the private sector.

- With which external organization(s) is the PII shared, what information is shared, and for what purpose?
  - Not Applicable. PII is not shared.

- Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, provide the SORN ID in use for this system. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.
  - Not Applicable. PII is not shared. Collected information is published on a public website, but only after PII is identified and redacted.

- How is the information shared outside the Department and what security measures safeguard its transmission?
  - Not Applicable.

- How is the information transmitted or disclosed?
  - Not Applicable.

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?
  - Not Applicable.

- How is the shared information secured by the recipient?
  - Not Applicable.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?
  - Not Applicable.

- Privacy Impact Analysis
  - Not Applicable.

1.7 NOTICE

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

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix or be prepared to provide a copy of the notice during an audit request. 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 Notice. If notice was not provided, please explain.
  - As noted above, in most cases, submission of PII will be inadvertent. Date of birth will be converted to age and the DOB will not be retained in the ITA system. OSHA will also include a proactive statement instructing respondents not to include PII in their narratives.

- Do individuals have the opportunity and/or right to decline to provide information?
  - No, response to the collection is mandatory.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
  - No. As noted above, employers are required to enter specific information about an employee's injury and illness on the recordkeeping forms. Also as explained above, the electronic submission of certain information from the recordkeeping forms is mandatory. Individual employees do have the right to request that an employer not enter their names on the source forms for specific types of injuries and illness. (See 1904.29(b)(6)). However, as stated above, the system will not collect data from the name fields of the source forms.

- Privacy Impact Analysis

  The "Privacy and Security Statement" link is on the bottom of all ITA webpages. It's possible that users won't click on the link and view the policy. However, the covered establishments are fully aware of the information collection since they are specifically entering data from their own recordkeeping forms.

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

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

- What are the procedures that allow individuals to gain access to their own information?
  - Employees and their representatives already have access to injury and illness records that are maintained by their employers at the workplace under 29 CFR 1904.35. Employees also have access to injury and illness information submitted through the ITA once OSHA publishes the data on its public website. In addition, individuals have access to the submitted injury and illness data through the FOIA process.

- What are the procedures for correcting inaccurate or erroneous information?
  - Covered establishments can edit the current year's data in the ITA through their ITA accounts. They can also request edits of previous years' data through the OSHA ITA Help Desk.

- How are individuals notified of the procedures for correcting their own information?
  - Direction on how to edit data are provided in Job Aids posted on the OSHA ITA webpage and through enquiries submitted to the ITA Help desk.

- If no formal redress is provided, what alternatives are available to the individual?
  - See above.

- Privacy Impact Analysis
  There are no risks associated with the redress information. Correction is accomplished by the individual submitting correct information to access the specific service.

1.9 TECHNICAL ACCESS AND SECURITY

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

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)
  - Only pre-approved OSHA users have access to the system based on their approved profile and associated rights.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA or be prepared to provide copies during an audit request
  - Yes. Only pre-approved OSHA users with have access to the system based on their approved profile and associated rights. Their role will be limited to application technical support.

- Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.
  - Yes.
  - ITA has built in role based access to the application data that is granted based on the approve account request forms that specifies the associated role; general user or system administrator.

- What procedures are in place to determine which users may access the system and are they documented?
  - Users are granted access only after completing and signing an account request form and it is received from an authorizing security manager indicating the user's role and assigned reporting office(s). The procedures are documented in the ITA Access Control Policies and Procedures.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often is training provided. Provide date of last training.
  - Each user is required to review and sign the Rules of Behavior at the time of account creation. All DOL employees and contractors are required to take the Training offered through DOL's Training Portal - LearningLink. Verification and audit is done using LearningLink reports.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?
  - DOL-wide Information Systems Security and Privacy Awareness Training is mandatory for all personnel connecting to the network or has access to OSHA data. Additionally, personnel with security responsibilities are required to complete role-based training.

- What auditing measures and technical safeguards are in place to prevent misuse of data?
  - NIST 800-53 Security Controls, Homeland Security Presidential Directive 12 (HSPD-12) and Identity Verification which are used for personnel security and Database auditing is implemented.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?
  - Yes. The latest ITA Security Controls Assessment Plan was signed in June 2023 and is currently being executed.

- Privacy Impact Analysis
  - OSHA Controlled Unclassified Information (CUI) is protected utilizing best security practices and redaction is employed for hard copies. NIST 800-53 Security Controls are implemented for risk mitigation, security safeguards against risks, unauthorized access or use, destruction, modification and unintended or inappropriate disclosure.

1.10 TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, biometrics, and other technology.

- Was the system built from the ground up or purchased and installed?
  - The system was built from the ground up.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.
  - The design considerations included the DOL guidelines specified in the SDLCM manual.
  - There are specific vetting processes, including OMB approved forms to collect data.
  - Database and application design process includes ensuring data integrity, privacy and security; this includes role-based user accounts to limit only appropriate users to have access to specific data.

- What design choices were made to enhance privacy?
  - Role based user accounts are used to limit access.

- For systems in development, what stage of development is the system in, and what project development life cycle was used?
  - Dev environment.

- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?
  - No.

1.11 DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

OSHA has completed the PIA for Injury Tracking Application which is currently in development. OSHA has determined that the safeguards and controls for this moderate system will adequately protect the information and will be referenced in Injury Tracking Application System Security Plan.

OSHA has determined that it is collecting the minimum necessary information for the proper performance of a documented agency function.

1.12 PIA SIGNATURE PAGE

Responsible Officials

Christopher Mace
System Owner

CHRISTOPHER MACE Digitally signed by CHRISTOPHER MACE
Date: 2023.06.29 09:54:34 -04'00'

Signature of System Owner

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for ☐ Federal employees, ☐ Contractor staff, ☐ Members of the Public {Check all that apply}

- ☐ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☐ First name ☐ Middle initial and/or ☐ Last name
- ☐ Name suffix such as Jr. Sr., etc.
- ☒ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☐ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ☐ Residential address
- ☐ Personal phone numbers (e.g., phone, fax, cell)

- ☐ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address
- ☒ Business address
- ☒ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☒ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☐ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☐ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?
  - No

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?
  - Not applicable.