U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

PRIVACY IMPACT ASSESSMENT

OSHA INJURY TRACKING APPLICATION (ITA)

VERSION 1.0

NOVEMBER 17, 2022

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/17/22	**ITA PIA_Nov172022**	**DSAM**	**Initial Draft**

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

The OSHA Injury Tracking Application (ITA) is the system that provides employers the means to meet the electronic reporting requirements contained under 29 CFR Part 1904.41. Specifically, employers that meet defined establishment size and industry criteria are required to electronically report to OSHA information from their occupational injury and illness records. 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. ITA does not collect PII data as defined by the Department of Labor (DOL).

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.

ITA only collects company information in a numeric form which is then calculated into percentages for that company. No information on individuals is entered into the system for collection and analysis.

The ITA System resides on a three-tiered architecture comprising of the web layer, application layer and database servers. This system is hosted at the DOL's database center in the Equinix facility in Ashburn, VA, on a fully virtualized and highly available server infrastructure, with a segregated production, staging, test and deployment environments that support the software development lifecycle.

1.2 CHARACTERIZATION OF THE INFORMATION

ITA collects and maintains annual injury information in identifiable form from business entities. Business with 200+ employees are required to submit the following information on an annual basis.

- Business Entity
  - EIN (not required)
  - Company Name
  - Company Address
  - NAICS
  - Size (number of company employees)
  - Government (Yes or No)
  - 300A Status (Submitted/Not Submitted)

- From whom is information to be collected?
  Data is collected from business entities, entity submitted numeric data on the annual number and type of injuries and deaths that occurred the previous year.
  - Business Summary for the Filing 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

- Why is the Information being collected?
  The information is being collected to help OSHA track the number and type of injuries, hours/days lost to injuries and number of deaths by company and type of company.

- What is the PII being collected, used, disseminated, or maintained?
  - Individual names and identifiers associated with their medical information.

- How is the PII collected?
  - The PII is being potentially received by members of the public through a narrative.

- How will the information collected from individuals or derived from the system be checked for accuracy?
  - No individual information is collected. Company annual injury numbers in a total number form is the only information collected.

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?
  - Submission of the data is required by 29 CFR Part 1904.41

- Privacy Impact Analysis
  Privacy risks are low because PII is not entered into the system. PII may be inadvertently received from the public.

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. ITA does not collect PII.

- Describe all the uses of the PII
  - The date of birth will be used to calculate the age of the injured or ill worker which in turn will be made publicly available. This data will not be associated with any individual personal identifiers. Note that the DOB will not be retained in the system. Any other submitted PII will be inadvertent and not used or published.

- 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. OSHA also intends to classify and publish the data using the BLS OIICS coding system for stakeholder analysis. 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.

- 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

  Has the retention schedule been approved National Archives and Records Administration (NARA)?
  - No

- 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?
  - Convert DOB to age and delete DOB

- 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).

- 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 of 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.

- 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.

- 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, submission of PII will be inadvertent, OSHA does not intend to collect PII. A date of birth will be converted to age and the DOB will not be retained. OSHA will also include a proactive statement instructing respondents not to include PII in their narrative.

- 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, but as noted, any submission of PII will be inadvertent.

- Privacy Impact Analysis

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

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?
  - Workers are provided access to the records that are located at their place of employment under 29 CFR part 1904.35. Workers will have access to the information provided to OSHA through the ITA when the Agency publicly posts it. Individuals will also have access to the data through the FOIA process.

- What are the procedures for correcting inaccurate or erroneous information?
  - Respondents can edit the current year's data in the ITA through their ITA accounts. Respondents can request through the OSHA Help Desk to edit previous years' data.

- 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 training is 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. Security Assessment and Authorization will take place early 2023.

- 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 process to include 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 to be completed by February 1, 2023.

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: 2022.11.21 07:28:02 -05'00'

_____

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.