U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

PRIVACY IMPACT ASSESSMENT

OSHA TECHNOLOGY INFORMATION SYSTEM (OTIS)

VERSION 1.8

January 24, 2024

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
2/2021	**FY21_OTIS PIA, 1.8**	**C. Lavender**	**Initial**

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
1/2024	OTIS PIA, 1.8	Yenyin Chin

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

The OSHA Technology Information System (OTIS) is the umbrella system that encompasses a collection of minor business applications that support OSHA's mission to ensure safe and healthful working conditions for America's working men and women. These applications perform various functions for OSHA that include case management activities, health sampling and analysis, injury and complaint reporting, maritime crane certification and the management of OSHA's partnership program among others.

OSHA Technology Information System (OTIS) comprises of the following applications:

- Chemical Exposure Health Data (CEHD)
- Draft.OSHA.gov
- eCorrespondence Administration (eCor)
- Event Forum
- Extranet Account Administration
- Intranet.OSHA.gov/Extranet.OSHA.gov website including web content and web forms that collect information and store it in a database, and data search
- Maritime Crane (MC)
- Medical Access Order (MAO)
- OITSS User Admin Tool (OUAT)
- OSHAPedia
- OSHA Account Certification Tool (O-ACT)
- OSHA Data Initiative (ODI)
- OSHA Legacy Data (OLD)
- OSHA Medical Examination Tracking Application (OMETA)
- OSHA Multisite (Drupal CMS)
- OSHA Office of Training and Education Course and Trainer Database (OTE Admin) formerly DTE Admin
- OSHA Strategic Partnership Automated Data System (OSPADS)
- OSHA Public Inspection Searches
- Severe Injury Report (SER)
- SitePro Content Management System (CMS)
- State Plans Application (SPA)
- Subversion
- USEUOSH.org (EUUSOSH.org) website including web content
- Voluntary Protection Programs (VPP) Automated Data System (VADS)
- VPP Forms
- Whistleblower
- www.OSHA.gov website including web content and web forms that collect information and store it in a database including (but not limited to):
    - eCorrespondence Form
    - Mechanical Power Presses Form
    - OSHA eComplaint Form (OSHA7)
    - OSHA Publication Order Form

    - Safe + Sound Event Form and Recognize Participation Forms
    - Web Forms Module
    - Website Error Report Form
    - Whistleblower Complaint Form
- www.Whistleblowers.gov website including web content

OTIS and OBIS
The OTIS and OBIS Systems reside on a three-tiered architecture comprising of the web layer, application layer and database servers. This system is hosted at the DOL database center within the Equinix facility in Ashburn, VA, on a fully virtualized and highly available compute and storage infrastructure, with segregated production, staging, test and deployment environments that support the software development lifecycle.

- The database servers are hosted on an Oracle RAC infrastructure built on a Sun SPARC T7 hardware cluster.
- The Middle Tier application servers comprise of Solaris logical server partitions on a Sun SPARC T7 hardware server pool.
- The Web servers comprise of RedHat virtual servers hosted on VMWare ESXi hosts. The applications that are accessible within the DOL network reside behind a set of Cisco ASA firewalls, while the public facing web applications are hosted on virtualized web servers in the DMZ

OSHApedia
The OSHApedia system resides on two servers (one for production and one for staging), each of which consists of a web server (Apache HTTPD) and a database (MariaDB, a MySQL clone). The system is hosted at Data Center 1 in Ashburn, VA, on a fully virtualized infrastructure with segregated production and staging environments. Both servers are Red Hat Enterprise Linux servers hosted on VMware ESXi hosts. The application is only accessible within the DOL network and resides behind a set of Cisco ASA firewalls. There is no public access to the application.

DDP
OSHA Multisite are now integrated into the OTIS security boundary and hosted on the Digital Data Platform (DDP) in the Azure cloud environment. OSHA Multisite consists of a Drupal 10 CMS containing OSHA.gov, Whistleblowers.gov and USEUOSH.org websites, forms, and databases. OSHA Multisite is one of many tenants/projects on the DOL Digital Platform (DDP). The platform utilizes the following MS Azure virtual infrastructure and is maintained by OCIO DDP platform team.

1.2 CHARACTERIZATION OF THE INFORMATION

OTIS collects and maintain information in identifiable form from DOL federal employees, other federal employees, federal contractors, and members of the public.

- From whom is information to be collected?
  Data is collected from individuals or business entities, complainant provides information when filing a complaint, and users submit non-sensitive PII in order to use specific services.

- Why is the Information being collected?
  The information is being collected to help OSHA enforcement whistleblower and cooperative program officials contact individuals and companies for investigation and necessary follow-ups. OSHA Certified Safety and Health Officials (CSHOs) collect, report, and review PII data gathered in the field from employee exposure assessments, chemical sampling, and emergency response activities such as hurricanes, tornados, and other nationally significant incidents.

- What is the PII being collected, used, disseminated, or maintained?
  - PII information collected may include the individual's name, address, phone number(s), email addresses, general contact information, and employee ID numbers.
  - Members of the public PII information may include name, home address, work address, phone number(s), email addresses, and basic medical information (Primary physician name, Clinic or Hospital POC, etc.).}

- How is the PII collected?
  - OSHA Information System data transfers.
  - Verbal interview entered onto paper form then inputted via OSHA Intranet web-based forms.
  - During system updates by OSHA field staff from inspections and investigations. Complainants provide the information either orally or in writing, and then the information is entered into the OTIS Application(s).
  - Direct input via web-based forms

- How will the information collected from individuals or derived from the system be checked for accuracy?
  - Edit checks are in place within the application to ensure accuracy of data input. In addition, information may be verified by the investigator of the case/record.
  - Technical controls are in place as data is checked during submission on the form. The contact information is verified or rejected as the minor applications attempt to provide the requested services, some applications use automated means and some require human intervention

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?
  - Occupational Safety and Health Act, 29 U.S.C. §660
  - Surface Transportation Assistance Act, 49 U.S.C. §31105
  - Asbestos Hazard Emergency Response Act, 15 U.S.C. §2651
  - International Safe Container Act, 46 U.S.C. §80507
  - Safe Drinking Water Act, 42 U.S.C. §300j–9(i)
  - Energy Reorganization Act, 42 U.S.C. §5851
  - Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C.
  - §9610(a)–(d)
  - Federal Water Pollution Control Act, 33 U.S.C. §1367
  - Toxic Substances Control Act, 15 U.S.C. §2622

- Solid Waste Disposal Act, 42 U.S.C. §6971
- Clean Air Act, 42 U.S.C. §7622
- Wendell H. Ford Aviation Investment and Reform Act for the 21st Century, 49 U.S.C.
- §42121
- Sarbanes-Oxley Act, 18 U.S.C. §1514A
- Pipeline Safety Improvement Act, 49 U.S.C. §60129
- Federal Rail Safety Act, 49 USC §20109
- National Transit Systems Security Act, 6 USC §1142
- Affordable Care Act, 29 U.S.C. §218C
- Consumer Financial Protection Act, 12 U.S.C. §5567
- Consumer Product Safety Improvement Act, 15 U.S.C. §2087
- FDA Food Safety Modernization Act, 21 U.S.C. §399d
- Moving Ahead for Progress in the 21st Century Act, 49 U.S.C. §30171
- Seaman's Protection Act, 46 U.S.C. §2114

- Privacy Impact Analysis

  Privacy risks are low because of access, physical and logical security controls that are implemented.

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.

- Describe all the uses of the PII
  - Used for OSHA investigations, inspections, accidents and fatality reporting.
  - Required to contact complainants and responders during the course of investigations.
  - Non-sensitive PII is used for contacting users for mailing of OSHA publications and responding to online complaints.
  - Any PII data is redacted prior to sharing in public facing websites or in FOIA request responses.
  - Used to contact employees in cases where high chemical exposure was experienced during chemical sampling assessments

- What types of tools are used to analyze data and what type of data may be produced?
  - Basic automated data checking during submission. No data is reused, produced in another form, or displayed

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
  - No

- If the system uses commercial or publicly available data, please explain why and how it is used.
  - Postal Zip Code data; A table is used to validate all zip codes that are entered.
  - Data is used only for the purpose of contacting the requesting web users.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?
  - No

- Privacy Impact Analysis
  - OTIS 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?
  - Review business retention requirements.
  - Decommissioning of applications when they are no longer needed.

- 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.
  - SSL for encryption, LDAP for user authentication and application authorization through defined roles and privileges.

- 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 PII data is used by authorized OSHA area, regional and national office employees.
  - Information is shared within OSHA Office of Occupational Medicine and Nursing (OOMN) employees and other internal agencies as required.

- How is the PII transmitted or disclosed?
  - Transmitted via secured network resources.

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?
  - Yes.

- Privacy Impact Analysis
  - If information is provided under FOIA, sensitive data is redacted in the data file; data is encrypted. Possible low level risk include emails which are not encrypted could be intercepted; however these are only sent to specific system owners or gatekeepers all internal to DOL. Exception to this process is the online complaint form in which emails are sent externally to OSHA state gatekeepers. PII contained in these emails are non-sensitive and publicly available.
  - Additionally, a database administrator, (DBA) could access the information using SQL statements. However, DBAs are governed by DOL and OSHA policy regarding disclosure and separation of duties

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? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.
  - 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.
  - Yes.

- Do individuals have the opportunity and/or right to decline to provide information?
  - Yes.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
  - Yes.
  - The individual is protected under the Privacy Act. The data is used only as part of an investigation and individuals waive the right to consent to particular uses of the information, once they submit a complaint. An individual has the right not to provide PII and by submitting their information they automatically consent to its use according to the DOL web Privacy and Security Statement

- Privacy Impact Analysis
  - Individuals are notified of the fact that OSHA electronically manages the data they have voluntarily submitted; however, as this data is for internal and exclusively government use, and very limited disclosures (to respondents, other agencies, and Congress) are mandated by law, there is minimal risk. This risk is mitigated by controlling access to the system.
  - 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?
  - Any request for a record of the Department of Labor must conform to the DOL's Freedom of Information Act (29 CFR Part 70) or Privacy Act (29 CFR Part 71) regulations. Such a request must be in writing and sent by mail, delivery service or facsimile or by email to foiarequest@dol.gov.

- What are the procedures for correcting inaccurate or erroneous information?
  - In the case of inspections and investigations, the user notifies the Regional Office that performed the inspection or investigation.
  - For some minor applications, if an individual enters incorrect information they will not receive the services of the minor application collecting it. They will have to reenter their information again to obtain access to those services.
  - The individual notifies the CSHO that performed the initial verbal interview to correct inaccurate information.

- How are individuals notified of the procedures for correcting their own information?
  - Individuals are notified verbally and are provided a written statement for their review.

- If no formal redress is provided, what alternatives are available to the individual?
  - The user may contact an OSHA office.
  - User will have to re-enter their information again to obtain access to services.
  - The individual may contact the CSHO.

- 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.
  - Each application 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 OTIS 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.
  - 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). They are required to review and sign the ROBs. Training is conducted in accordance with the Department policy.

- 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 annually

- What auditing measures and technical safeguards are in place to prevent misuse of data?
  - All user accounts are reviewed and recertified twice a year to ensure only active users have appropriate privileges to the system.
  - Application and system users are required to have prescribed training on handling of PII data prior to gaining access to the DOL systems and refresher training every year.
  - System administrator(s) conduct monthly audit log reviews.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?
  - Yes
  - March 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.
  - There are specific vetting process to include OMB approved forms to collect data.
  - Database and application design process includes insuring 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?
  - Not Applicable.

- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?
  - Not Applicable.

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?

OASAM has completed the PIA for OTIS, which is currently in operation. OSHA has determined that the safeguards and controls for this moderate system adequately protect the information.

OASAM 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: 2024.03.05 08:16:19 -05'00'

Signature of System Owner

Adrienne Ramirez
Privacy Officer, PO

Signature of Privacy Officer

Christopher Lavender
Information System Security Manager, (ISSM)

Signature of ISSM

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?
  - Yes.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?
  - The data is used only as part of an investigation and individuals waive the right to consent to particular uses of the information once they submit a complaint or request. An individual has the right not to provide PII and by submitting their information, they automatically consent to its use according to the Privacy and Security Statement.