



U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

**OFFICE OF LABOR-MANAGEMENT
STANDARDS LABOR
INVESTIGATIONS VISUALIZATION &
IN-TIME ANALYTICS SYSTEM
(OLIVIA) PRIVACY IMPACT
ASSESSMENT**

VERSION 1.0

Dec. 05, 2023



DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
12/5/2023	OLMS OLIVIA PIA FY24	T. Colson	Initial Draft

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers



TABLE OF CONTENTS

1	PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE	4
1.1	Overview	4
1.2	Characterization of the Information	4
1.3	Uses of the PII	5
1.4	Retention	6
1.5	Internal Sharing and Disclosure	7
1.6	External Sharing and Disclosure	8
1.7	Notice	9
1.8	Access, Redress, and Correction	10
1.9	Technical Access and Security	11
1.10	Technology	12
1.11	Determination	13
1.12	PIA Signature Page	14
	Appendix A: Definitions for PII and PII Elements this system collects	15 - 16



1 PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

The Office of Labor-Management Standards (OLMS) administers and enforces most provisions of the Labor Management Reporting and Disclosure Act (LMRDA). The LMRDA was enacted primarily to ensure basic standards of democracy and fiscal responsibility in labor organizations representing employees in private industry. Unions representing U.S. Postal Service employees became subject to the LMRDA with the passage of the Postal Reorganization Act of 1970.

Under the LMRDA, labor unions and others are required to file annual financial reports with OLMS and these reports are required to be made available for review by any interested party. In 2002 OLMS implemented electronic filing for labor organization annual reports (LM-2, 3, and 4). OLMS also created an Internet public disclosure system that provides public access to filed labor organization reports and to a searchable database of information for those reports. In 2010 OLMS implemented a modernized Electronic Filing System (EFS) which is a browser based application that provides users access to the required reporting forms via their current web browser and web submission of completed forms through the same browser. OLMS also discloses data filed on the LM-10, LM-20, LM-21, and LM-30 reports in an online searchable database. The various tasks of OLMS are managed and supported by OLMS Labor Investigations Visualization & In-time Analytics System (OLIVIA).

OLIVIA was initiated to support the President's Management Agenda to expand electronic government by automating a paper-based reporting and public disclosure system under the LMRDA. It also ensures compliance with the Government Paperwork Elimination Act, P.L. 105-277, Title XVII, by making required forms available for electronic submission

This Privacy Impact Assessment (PIA) report seeks to identify the essential components of the OLMS OLIVIA to ensure that personally identifiable information (PII) is protected by security procedures and controls commensurate with the sensitivity of the information.

1.2 CHARACTERIZATION OF THE INFORMATION

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

Specify whether the system collects personally identifiable information (PII) on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

- What are the sources of the PII in the information system?
Under the LMRDA, labor union members file complaints with OLMS concerning misbehavior of Union Officers and Union Members. When the complaint is filed OLMS collects PII information on the complainant to use as reference in relationship to the complaint investigative process.



- What is the PII being collected, used, disseminated, or maintained?
Name, mailing address, phone number, and business address. All information collected is non-sensitive PII.
- How is the PII collected?
Non-sensitive PII is collected manually at time of input the complaint is filed.
- How will the information be checked for accuracy?
The data is reviewed on an annual basis.
- What specific legal authorities, arrangements, and/or agreements defined the collection of information?
Labor-Management Reporting and Disclosure Act of 1959.
- Privacy Impact Analysis
All OLMS employees receive annual computer security awareness training which includes information concerning each employee's responsibility to safeguard the privacy of the information received by OLMS. All employees are also responsible to be familiar with and abide by the OLMS Rules of Behavior which address proper security measures each employee must follow to be granted access to OLIVIA and the information it contains. OLMS complies with all Federal guidelines concerning least privilege policies. OLIVIA users are granted only the access they need to perform their duties and nothing more.

1.3 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.
Internal use only PII information is used to identify previous complainants and their investigative history with OLMS.
- What types of tools are used to analyze data and what type of data may be produced?
A visual analysis of the data and the data produced is the history of reporting of the complainant for investigative files.
- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
Yes, we will be updating contact information or potentially starting a new complaint summary.
- If the system uses commercial or publicly available data, please explain why and how it is used.
Not applicable



- Privacy Impact Analysis

The non-sensitive PII is read only information. And the data is protected by the case management platform. The impact is minimal.

1.4 RETENTION

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

- How long is information retained in the system?
Non-sensitive PII is retained indefinitely.
- Has the retention schedule been approved by the DOL agency records officer and the National Archives and Records Administration (NARA)?
Approval of OLMS records retention schedule was granted by a DOL Records Officer and a National Archives and Records Administration official in January 2023.
- Privacy Impact Analysis
Current policy requires effectively maintaining the security of non-sensitive PII gathered by OLMS. The current records retention schedule will be reviewed and modified as necessary if there were any significant changes to the OLMS processes in the future.



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?
This information is not shared internally with any organization(s).
- How is the PII transmitted or disclosed?
N/A
- Privacy Impact Analysis.
Non-sensitive PII gathered by OLMS is not shared internally with any offices and/or organizations.



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?

No information is 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, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.

N/A

- How is the information shared outside the Department and what security measures safeguard its transmission?

N/A

- Privacy Impact Analysis

N/A



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?
At the point of collection of non-sensitive PII, the complainant has the option to not provide their information.
- Do individuals have the opportunity and/or right to decline to provide information?
Yes, if the complainant chooses to remain anonymous, they can refuse to provide the non-sensitive PII.
- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
Yes. They exercise their right by stating so at the time of filing of the original report.
- Privacy Impact Analysis
The intake of the PII is done verbally by an individual who is trained to properly manage the information provided. The rights of the complainant are identified and conveyed in accordance with the Privacy Policy for managing non-sensitive PII.



1.8 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 information?
The complainant contacts their local district office to gain access to their information.
- What are the procedures for correcting inaccurate or erroneous information?
OLMS will reach out to the complainant, or the complainant will reach out to OLMS and the information will be corrected.
- How are individuals notified of the procedures for correcting their information?
OLMS staff will provide the guidance and the time of collection.
- If no formal redress is provided, what alternatives are available to the individual?
The complainant calls the OLMS local district office.
- Privacy Impact Analysis
OLMS continually reviews the information received from complainants in their reports filed. If errors are found, they are corrected immediately.



1.9 TECHNICAL ACCESS AND SECURITY

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

- What procedures are in place to determine which users may access the system and are they documented?
OLMS OLIVIA users are required to sign the OLMS ROB prior to granting access to the system. The OLMS/OLIVIA IT Rules of Behavior states that the policy of least privileges is in place and enforced when granting OLMS personnel access to the OLIVIA database. OLIVIA user access is reviewed on a semi-annual schedule by the OLMS Federal Lead to ensure compliance with these regulations.
- Will Department contractors have access to the system?
As stated in the OLMS/OLIVIA IT Rules of Behavior, OLMS developers/contractors are not permitted access to the OLIVIA production system.
- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?
All OLMS computer users, federal employees and contractor staff, are required to complete the annual computer security training provided by the DOL.
- What auditing measures and technical safeguards are in place to prevent misuse of data?
The OLMS/OLIVIA IT Rules of Behavior states that the policy of least privileges is in place and enforced when granting OLMS personnel access to the OLIVIA database. OLIVIA user access is reviewed on a semi-annual schedule by the OLMS ISO to ensure compliance with these regulations.
- Privacy Impact Analysis
By enforcing the Rules of Behavior, OLMS can safeguard data collected from labor organizations. As stated by both OLMS and DOL, it is imperative of all employees that they be aware of their security responsibilities to protect Federal information and Federal information systems. Toward this goal, DOL provides annual computer security training for all employees and contractors entrusted with access to Federal computer systems and information.



1.10 TECHNOLOGY

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

- What stage of development is the system in, and what project development life cycle was used?

OLIVIA is in the pre-production phase of the computer security lifecycle as defined in the DOL System Development Lifecycle Management Manual (SDLCMM).

- Does the project employ technology which 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?

OLMS has completed the Privacy Impact Analysis for OLIVIA which is currently in pre-production. OLMS has determined that the safeguards and controls for this moderate computer system adequately protect the information.

OLMS 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

Avieon Morgan

Signature and Date 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 plate, 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? No action is taken currently. These activities will take place by request of the person whose PII is maintained in the system.