



PRIVACY IMPACT ASSESSMENT

Effective Date: October 8, 2026

DOL- Office of Inspector General
Office of Inspector General Warehouse and
Learning System (OWLS)

- ☒ Concurrence of Senior Agency Official for Privacy
- ☐ Non-concurrence of Senior Agency Official for Privacy

BRAYE CLOUD Digitally signed by BRAYE
CLOUD
Date: 2026.10.08 09:23:08 -04'00'

Braye Cloud, Senior Agency Official for Privacy (SAOP)

Deputy Assistant Secretary for Operations

Office of the Assistant Secretary for Administration & Management



OVERVIEW & GENERAL INFORMATION

As required by the E-Government Act of 2002 (as amended) and OMB Memorandum M-03-22, OIG has developed this Privacy Impact Assessment to describe:

1. The information to be collected with a particular focus on personally identifiable information (PII);
2. Why the information is being collected including the legal authority for the information collection;
3. The intended use of the information;
4. With whom the information will be shared (such as internal uses with other DOL component agencies or another federal agency);
5. What notice is provided to individuals, what opportunities are given to individuals to consent to particular uses of the information, how individuals can grant consent, and what opportunities individuals have to decline to provide information;
6. How the information will be secured with administrative and technological security controls;
7. Whether a *system of records* is being created under the Privacy Act, 5 U.S.C. 552a; and
8. The analysis of privacy risk associated with the collection, use, storage, and dissemination of information and practices that have an impact on privacy.

Name of System (and Acronym, if applicable)

Office of Inspector General Warehouse and Learning System (OWLS)

Location of the System

OWLS is a data warehouse system located in the Equinix Datacenter TFG308 in Ashburn Virginia and is a Major Application running on the OIG GSS. Contained within the OWLS is a collection of highly customized analytical modules that assist auditors and investigators in identifying fraud, waste, and abuse. This development strategy eliminates the need for constant, ongoing integration of various software application technologies by providing one consistent, fully integrated analytical software platform.

Brief Description of the System

The Office of Inspector General Warehouse and Learning System is in support of the missions of the OIG Program Offices, primarily the Office of Investigations (OI), Division of Advanced Technology and Analytics (OI/DATA), and Office of Audit Business Intelligence Division (BID) to improve the efficiency and effectiveness of their work by incorporating data analytics. The Data Warehouse is a comprehensive computing environment designed and dedicated to support business intelligence activities such as reporting, and data analysis which enables OIG to consolidate and analyze data from various systems and provides a single version of truth for better decision-making.



- OWLS' manual data ingest process extracts, translates, and loads records from the following Department systems of records: OWCP - DOL Office of Workers' Compensation Programs Systems of Records
 - DOL/OWCP-2, Office of Workers' Compensation, Black Lung Benefits Claim File
 - DOL/OWCP-3, Office of Workers' Compensation Programs, Longshore and Harbor Workers' Compensation Act Case Files
 - DOL/OWCP-4, Office of Workers' Compensation Programs, Longshore and Harbor Workers' Compensation Act Special Fund System
 - DOL/OWCP-6, Office of Workers' Compensation Programs, Longshore and Harbor Workers' Compensation Act Claimant Representatives
 - DOL/OWCP-7, Office of Workers' Compensation Programs, Physicians and Health Care Providers Excluded under the Longshore Act
 - DOL/OWCP-8, Office of Workers' Compensation Programs, Physicians and Health Care Providers Excluded under the Federal Employees' Compensation Act
 - DOL/OWCP-9, Office of Workers' Compensation Programs, Black Lung Automated Support Package
 - DOL/OWCP-11, Office of Workers' Compensation Programs, Energy Employees Occupational Illness Compensation Program Act File
 - DOL/OWCP-12, Office of Workers' Compensation Programs, Physicians and Health Care Providers Excluded under the Energy Employees Occupational Illness Compensation Program Act
- Government-Wide Systems of Records
 - DOL/GOVT-1, Office of Workers' Compensation Programs, Federal Employees' Compensation Act File
 - GSA/GOVT-3-Travel Charge Card Program
- ETA- DOL Employment and Training Administration Systems of Records
 - DOL/ETA-7, Foreign Labor Certification System and Employer Application Case Files
 - UI Related Programs data from State workforce agencies (SWAs): UI Programs Authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 (Federal Pandemic Unemployment Compensation (FPUC), Pandemic Unemployment Assistance (PUA), Pandemic Emergency Unemployment Compensation (PEUC)), and FEMA's Lost Wages Assistance Program (LWAP)
 - DOL-OIG receives data extracts regarding the State's Unemployment Insurance (UI) Program. The information is to be provided for all claims regardless of status, including but not limited to, active, locked, cancelled, incomplete, and paid claims
- MSHA - DOL Mine Safety and Health Administration Systems of Records
 - DOL/MSHA-1, Mine Safety and Health Administration Standardized Information System (MSIS)
- ADJBDS - DOL Adjudicatory Boards Systems of Records
 - DOL/ABJBDS-1, DOL Appeals Management Systems (AMS)



Purpose of the System:

☐ Program administration	☐ Employee or customer satisfaction surveys
☐ Computer Matching Program	
☐ Administering human resources programs for DOL or federal government personnel	☐ Improve Federal services online
☐ Litigation	☐ Promote information sharing initiatives
☒ Criminal law enforcement activities	☐ Civil law enforcement activities
	☐ Other.

This System is operated by:

- ☒ Component agency: OIG Office of Investigation (OI), Office of Audit Business Intelligence Division (BID)
- ☐ Contractor

For a system operated by a contractor, the contract or other acquisition-related documents includes privacy requirements:

- ☐ Yes
- ☐ No

This PIA is being conducted for:

- ☐ A new information system or project that collects, maintains, or disseminates information in identifiable form.
- ☐ A new collection of information subject to the Paperwork Reduction Act because it is for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government in the scope of their employment).
- ☐ A change to the PII Confidentiality Impact Level (NIST SP 800-122) or System Security Categorization (NIST SP 800-60).
- ☒ An existing system subject to a periodic review at the 5-year mark.
- ☐ An existing system with significant changes that create new privacy risks.

The following are the significant changes that create new privacy risks:

- ☐ Changed information collection authorities.
- ☐ Changed business processes.



- ☐ Conversion of paper-based records to electronic systems.
- ☐ Anonymous to Non-Anonymous. This is when functions applied to an existing system change anonymous information into information in identifiable form.
- ☐ Significant System Management Changes. This is when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.
- ☐ Significant Merging. This is when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.
- ☐ New Public Access. This is when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.
- ☐ Commercial Sources. This is when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources.
- ☐ New Interagency Uses. This is when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.
- ☐ Internal Flow or Collection. This is when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.
- ☐ Alteration in Character of Data. This is when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).
- ☐ Other.

The class(es) of users who will have access to the system are:

- ☐ General Public
- ☒ Contractors
- ☒ Government Employees
- ☐ Other.

1. INFORMATION IN THE SYSTEM

OIG collects certain types of information from certain sources using particular methods to collect the information, as identified below.

1.1. The information that is collected, used, maintained, or disseminated in connection with the system is:

☒ Name/Former Name	☒ Date of Birth	☐ Maiden Name	☒ Place of Birth	☐ Citizenship
☒ Social Security number (including in truncated form)	☒ Driver's License	☐ Financial Account	☒ Taxpayer ID	☒ Passport Number
☐ Gender	☒ Telephone Number	☐ Criminal Record	☒ Education	☒ Age
☒ Financial Transaction	☒ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☒ Employee ID
☐ Credit Card	☐ Medical Record	☒ File/Case ID	☐ Financial Information	☐ Religion
☐ Alias	☒ Home Address	☐ Military Service	☐ Mother's Maiden Name	☒ Medical Information
☒ Email Address	☐ Marital Status	☐ Race/Ethnicity	☒ Occupation	☒ Work Email Address
☐ Job Title	☒ Salary	☐ Business Associates	☒ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☐ Work Address	☐ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☒ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☐ Weight	☐ Voice/Audio Recording	☐ Eye Color
☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☐ Height	☐ Retina/Iris Scans
☒ User ID	☒ IP Address	☒ Other PII: Billing records, Employer records, Department grantees, contractors, consultants, advisory committee members and other individuals receiving funds from the Department.		

1.2. The information is collected using the following methods:

- ☐ Website-based forms
- ☐ Paper forms
- ☐ Electronic forms
- ☐ Verbal collection
- ☒ No form - the information collected does not require a specific form

1.3. The source of the information is:

Directly from the Individual about Whom the Information Pertains		
☐ In Person	☐ Hard Copy: Mail/Fax	☐ Web-based (uploading through an app or website)
☐ Telephone	☐ Email	☐ Legal or other representative.
☐ Other.		

Government Sources		
☒ Within the Component Agency	☒ Other DOL component agencies, OSHA, OLMS, WHD)	☒ Other Federal Agencies
☒ State, Local, Tribal	☐ Foreign	☒ Other: State Workforce Agencies (SWA)

Non-government Sources		
☐ Public Organizations	☐ Private Sector	☐ Commercial Data Brokers
☐ Third Party Website or Application	☐ Other.	

1.4. Social Security numbers (SSN) are collected:

The Privacy Act of 1974 requires that when DOL requests that an individual provide a Social Security number, DOL must indicate whether that disclosure is mandatory or voluntary and by what statutory or other authority the number is being requested including what uses will be made of it.



Additionally, OMB Circular A-130 to the Heads of Executive Departments and Agencies regarding *Managing Information as a Strategic Resource* includes a requirement that DOL take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.

Finally, DOL policies permit component agency programs to collect, use, maintain, and disseminate SSNs only when required by law (e.g., statute, Executive Order, or upon approval of the SAOP or SAOP designee).

Will SSNs be collected for this system, whether directly or indirectly from the individual to whom the SSN applies?

- ☐ No
☒ Yes

1.4.1. If yes, the specific authority relied upon to collect SSNs?

Section 6(a)(1) of the Inspector General Act of 1978, (Pub. L. 95-452, § 1, Oct. 12, 1978, 92 Stat. 1101), authorizes The Inspector General to “have access to all records, reports, audits, reviews, documents, paper, recommendations, or other material available to the applicable establishment which relates to programs and operations”.

1.4.2. The purpose for the collection of SSNs and how the SSN will be used is as follows:

The SSN is already included in the documentation of racketeering and fraud investigation or audit activities to provide a record of interviews, witnesses, investigative targets, and audit details. The IG Act allows OIG to collect data from any and all DOL components data sets.

1.4.3. The following alternatives were considered in lieu of the collection of SSNs:

There is no alternative. The collection of SSNs is performed by other DOL, federal and local state agencies.

1.4.4. The alternatives were not selected because:

N/A

1.5. The information collected is subject to the Paperwork Reduction Act:

- ☐ Yes, some or all of the information is covered by the Paperwork Reduction Act.
- ☐ The information expected to be collected does not yet have an OMB control number but will be submitted for PRA approval.
- ☐ The information collected is part of an existing collection and the OMB control number for the collection is.
- ☒ No, the information collected is not subject to the Paperwork Reduction Act.



2. WHY THE INFORMATION IS BEING COLLECTED

2.1. Why is the information being collected?

The OIG Data Warehouse is a comprehensive computing environment designed and dedicated to support and improve the Offices of Investigations and Audit's ability to analyze stakeholder data and increase business intelligence, in support of investigative and audit activities.

2.2. The following are the specific legal authorities and/or agreements that permit the collection, use, maintenance, and/or dissemination of information (including any PII) by the system:

Pursuant to the Inspector General Act of 1978, (Pub. L. 95-452, § 1, Oct. 12, 1978, 92 Stat. 1101), as amended by Section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), authorizes the Inspector General to conduct audits and investigations that relate to the OIG's mission.

3. INTENDED USE OF THE INFORMATION

3.1. The information collected by the system is used in the following ways:

The PII is included in the documentation in support of investigative or audit activities to provide a record of interviews, witnesses, investigative targets, and audit details

3.2. The system aggregates or analyzes information to create new information:

- ☒ Yes
☐ No

4. INFORMATION SHARING AND ACCESS

4.1. Will OIG OWLS share data internally or externally?

- ☒ Yes, the PII in the system will be shared.
☐ No, The PII in the system will not be shared.

Internal Sharing:

Component Agency	Information Shared	Purpose
ETA	Unemployment Insurance Data	Shared in conjunction with EO "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos"



OCIO	Unemployment Insurance Data	Shared in conjunction with EO "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos"
------	-----------------------------	---

External Sharing:

Organization	Information Shared	Purpose	MOU or other Agreement
Various OIG agencies in federal government	Unemployment Insurance Information related to their agency	IG Act	Data Use Agreements
Pandemic Recovery Accountability Committee	Pandemic Unemployment Insurance Information	IG Act	MOU

4.2. Does OIG OWLS place a limitation on re-dissemination of PII shared with internal or external organizations?

Internal Sharing

- ☐ Yes, another DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII.
- ☒ No, another DOL component agency is not required to verify with the component agency operating the system before re-dissemination of PII.
Pursuant to Executive Order titled Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, dated March 20, 2025, the Department of Labor, Office of Inspector General (DOL-OIG) provided all unemployment insurance (UI) information within its possession to the Employment and Training Administration (ETA). Pursuant to DLMS 8-203, ETA should report all allegations of fraud, waste, abuse, mismanagement, or misconduct received from any source to DOL-OIG. However, ETA is not required to notify us of any re-dissemination of UI data.
- ☐ Not applicable, the component agency does not share PII with other DOL component agencies.

External Sharing

- ☒ Yes, the external agency or entity is required to verify with the DOL component agency before re-dissemination of PII.
Data use agreement and MOU requires notice of any duplication or dissemination of data shared to agencies.



- ☐ No, the external agency or entity is not required to verify with the DOL component agency before re-dissemination of PII.
- ☐ Not applicable, the component agency does not share PII with external agencies or entities.

4.3. Indicate whether the system connects with or receives information from any other systems authorized to process PII.

- ☐ Yes, this system connects with or receives information from another system(s) authorized to process PII.

If the answer to 4.3 is yes, provide the name of the system and describe the technical controls which prevent improper accessing of the PII while in transit.

- ☒ No, this system does not connect with or receive information from another system(s) authorized to process PII and/or BII.

5. NOTICE, CONSENT, AND OPPORTUNITY TO DECLINE TO PROVIDE INFORMATION

5.1. Indicate whether individuals will be notified if their PII is collected, maintained, or disseminated by the system.

- ☐ Notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.
- ☐ Notice is provided by a Privacy Act Statement and/or a Privacy Notice. The Privacy Act Statement and/or Privacy Notice can be found on the following forms or information collection instruments.
- ☐ Notice is provided by other means.
- ☒ Notice is provided by means of this Privacy Impact Assessment.

5.2. Do individuals have an opportunity to decline to provide PII?

- ☐ Yes, individuals have an opportunity to decline to provide PII.
- ☒ No, individuals do not have an opportunity to decline to provide PII.
OWLS is a database where aggregated PII is housed; it does not collect the information directly from the individual. Therefore, the individual is not given the opportunity to decline to provide PII.

5.3. Do individuals have an opportunity to consent to particular uses of their PII?

- ☐ Yes, individuals have an opportunity to consent to particular uses of their PII.



- ☒ No, individuals do not have an opportunity to consent to particular uses of their PII.
OWLS is a database that houses aggregated data, any possible opportunity or right to consent to provide information would not be possible since the information was not provided through this system.

5.4. Do individuals have an opportunity to review or update PII pertaining to them?

- ☐ Yes, individuals have an opportunity to review or update PII pertaining to them.
- ☒ No, individuals do not have an opportunity to review or update PII pertaining to them.
Not Applicable. The OWLS system is not accessible to the public; the collecting agency and systems will address this.

6. HOW INFORMATION IS SECURED

As required by the E-Government Act of 2002 and OMB Memorandum M-03-22, DOL imposes certain administrative and technological controls on each system that contains PII. Below, DOL describes whether it has conducted a risk assessment, the security controls to put in place to protect against that risk, and how those controls are implemented. DOL also describes how it continuously monitors the system to ensure that the controls continue to work properly, safeguarding the information. Individuals who have questions regarding the information below may reach out to DOL's Privacy Program at privacy@dol.gov.

6.1. Administrative controls for the system:

- ☒ PII is kept in a secured physical location.
Physical controls are implemented with encryption on VM Nutanix Cluster in a secured on prem location in Ashburn, Nutanix port security is enabled to allow in-bound/out-bound traffic from the OIG network only. Users must be granted access at each time to specific databases.
- ☐ All users signed a confidentiality agreement or non-disclosure agreement.
- ☒ All users are subject to a Code of Conduct that includes the requirement for confidentiality.
All users are subject to DOL and OIG Rules of Behavior.
- ☒ DOL Personnel (employees, contractors, interns, volunteers) receive **annual** training on privacy and confidentiality policies and practices.
All DOL Personnel must annually take the Cybersecurity and Privacy Awareness Training via LearningLink, training is tracked on the site for user completion.
- ☐ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices.
- ☐ DOL Personnel (employees, contractors, interns, volunteers) receive **system-specific** training on privacy and confidentiality policies and practices.
- ☒ Access to the PII is restricted to authorized personnel only.
Access is restricted to investigators and auditors use only. Supervisors are required to submit an account authorization form requesting access to OWLS.



- ☐ Appropriate NIST SP 800-53 Revision 4 security controls for protecting PII are imposed.
 - ☐ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.
- ☒ Appropriate NIST SP 800-53 Revision 5 security controls for protecting PII are imposed.

The controls were imposed through continuous monitoring using Risk Management Framework through annual security assessment

 - ☒ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.

The last SAR date for OWLS was completed August 2025. OWLS undergoes continuous monitoring annually where one third of its security controls and privacy controls are assessed. For FY25 a total of 45 controls with 289 Determine IF statements were assessed. 44 controls were identified as satisfied (implemented) with 1 control resulting as other than satisfied.
- ☒ There is one or more Plan of Action and Milestones (POA&M) associated with this system.

The completion of this PIA will resolve the existing POA&M.
- ☐ Contractors that have access to the system are subject to information security provisions in their contracts required by DOL policy.
- ☐ Contracts with customers establish DOL ownership rights over data including PII.
- ☐ Other.

6.2. Technological controls for the system:

- ☒ Access to the PII is being monitored, tracked, or recorded:

All access is monitored and controlled by a Firewall. Additional monitoring is recorded on user and system audit logs which is tracked and reviewed on a monthly basis
- ☐ User Log In Credentials
- ☒ Virtual Private Network (VPN)

Access is limited to only connection to OIG network through VPN currently using Zscaler
- ☐ Biometrics
- ☒ Encryption of Data at Rest

Encryption is built for both in transit and at rest into the system to account for the possible privacy risks.
- ☒ Firewall

A Firewall monitors and prevents unauthorized users from accessing OIG's internal network from the Internet. There are no public access accounts. All access is monitored and controlled by Firewall. Additional monitoring of access from the Internet is provided by Internet Service Provider sensors.
- ☒ Role-based Access Controls

The Branch of Database Management and Application (BDMA) team have administrative rights; all other OIG users are assigned rights per their individual roles. There are no public users on the system.
- ☒ Encryption of Data in Transit

Encryption is built for both in transit and at rest into the system to account for the possible privacy risks.
- ☐ Use Only for Privileged (Elevated Roles)



☐ Other.

6.3. Retention of Information

Information in the system is covered by an approved records retention schedule and monitored for compliance.

☐ Yes.

☐ No.

☒ A records retention schedule is in development.

A records schedule for OWLS is currently under development in coordination with the OIG Records Officer. A draft retention schedule is in progress and will move through the formal approval process. Each data set within OWLS may be subject to a different retention period, depending on its purpose and how the data is used.

Records are maintained in accordance with FISMA requirements and the OIG Records Management Policies and Procedures. Consistent with these policies, OIG Warehouse data will be destroyed or deleted when it is no longer needed for administrative, legal, audit, or other operational purposes.

The retention disposition for OWLS data is temporary and generally ranges from 10 to 20 years. Any historical data retained beyond these timeframes will be maintained only when required by legislation or justified by business need.

If there is an approved record retention schedule, is retention monitored for compliance to the schedule?

☐ Yes, retention is monitored for compliance to the schedule.

☐ No, retention is not monitored for compliance to the schedule.

☒ No, there is not an approved record retention schedule.

When information is no longer needed, it is disposed of by:

☐ Shredding or other physical destruction

☐ Overwriting

☐ Physical destruction of hardware, such as degaussing

☐ Deleting

☒ Other: Records will be shredded, deleted, or otherwise physically destroyed in accordance with OIG Records Management Policies and Procedures. However, until a formal retention schedule is approved and in place, all records are treated as permanent.

7. SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act of 1974 (Privacy Act) requires DOL to permit individuals to gain access to their records (including obtaining copies and requesting amendments to the records) and any information pertaining to the requesting individual which is contained in a "system of records" (a specifically defined term under the Privacy Act). Although many DOL Information Systems may contain PII, they are not all



required to have a SORN. For purposes of the Privacy Act, a system of records that requires a SORN refers to any group of any records under the control of DOL (including through a contractor) 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. Some systems of records under DOL's control may be exempt from some of the Privacy Act rights provided to individuals. DOL is identifying all of the SORNs applicable to this system so that individuals may review the SORNs for more detailed additional information.

7.1. This system is covered by one or more existing SORNs.

DOL/OIG-12, Office of Inspector General Warehouse and Learning System (OWLS).

7.2. This system:

- ☒ Does not require an additional SORN beyond those identified above.
- ☐ Does not require a SORN.
- ☐ Requires a new or additional SORN.
- ☐ Requires a modification to the following SORN(s).

Reason for Modifying SORN(s):

- ☐ A significant increase in the number, type, or category of individuals about whom records are maintained.
- ☐ A change that expands the types or categories of information maintained.
- ☐ A change that expands the types or categories of information maintained.
- ☐ A change that modifies the scope of the system.
- ☐ A change that modifies the purpose(s) for which the information in the System of Records is maintained.
- ☐ A change in the agency's authority to maintain the system, collect, use, or disseminate the records in the system.
- ☐ A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute.
- ☐ A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system.
- ☐ The addition or rescindment of a Privacy Act exemption.
- ☐ A new routine use or significant change to an existing routine uses that has the effect of expanding the availability of the information in the system.



8. ANALYSIS OF PRIVACY RISK

8.1. PII Confidentiality Impact Level from NIST Special Publication 800-122

Indicate the potential impact/harm that could result to the subject individuals and/or DOL if PII were inappropriately accessed, used, or disclosed.

- ☐ **Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- ☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- ☐ **High** – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

8.2. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

OWLS Users are required to take the Cybersecurity and Privacy Awareness Training each year via LearningLink. The training focuses on principles of cybersecurity, federal laws and regulations on Privacy and obligations for mishandling PII.

How Information is Acquired, Stored, and Shared

OWLS information is acquired from federal agencies, state agencies, local agencies and DOL. The information is stored on OIG DataWarehouse which is housed in a secure location in Ashburn VA. Information within the DataWarehouse is used to support the OIG mission, investigations and audits activities and is not shared outside the mission area.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

OIG relies on the data source to follow PII safeguarding best practices which are standard throughout the Federal government. Information is always encrypted at rest and in transit.

Protection against PII Breaches

Unauthorized Data Access:

OIG has Firewalls in place that monitors and prevents unauthorized users from accessing OIG's internal network from the Internet. There are no public or temporary access accounts for OWLS. All access is monitored and controlled by firewalls. Access requires multifactor authentication (MFA) to access the system. Users are granted the least privileged access for the performance of their roles and casefiles they are working on.

Potential Misuse of Data:

OIG provides users Rules of Behavior training in LearningLink. OIG maintains and reviews audit logs for OWLS user activities. The system has access and permission roles that prevent those without a need to know from accessing the database.

Protecting Against Insider Threats:

All OWLS users have an official need to know associated with the investigative case or audit case they are working on. Access is restricted to investigators and auditors use only. Supervisors are required to submit account authorization form requesting access to OWLS.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

Unauthorized Data Access: OIG has Firewalls in place that monitors and prevents unauthorized users from accessing OIG's internal network from the Internet. There are no public or temporary access accounts for OWLS. All access is monitored and controlled by firewalls. Access requires multifactor authentication (MFA) to access system. Users are granted the least privileges access for the performance of their roles. Potential Misuse of Data: OWLS has access and permission roles that prevent those without a need to know from accessing the database. OIG places a limitation on the information shared internally or externally whereby DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII or data. Protecting Against Insider Threat: All users have an official need to know associated with the user roles. User audit logs are also reviewed monthly to detect any anomaly or unauthorized activities.

Other:

Describe what the Component Agency has done to reduce this risk.

Any DOL internal agency such as ETA that data is shared with is responsible for their risk management and procedures. ETA follows their own procedures for privacy risks, as well as DOL wide procedures. Typically, our scope of data protection ends when it's provided to another party. Data transferred is encrypted. Thereafter agencies are now the stewards of this data and are responsible for it.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

N/A



Appendix 1. Artificial Intelligence (AI) and Machine Learning (ML)

To be completed by an information system that integrates an AI/ML component

Name the AI and or ML application?

Describe what the AI/ML is being used for?

Does the AI/ML component input, access, process, store, analyze, or generate outputs using any PII?

☐ Yes

☒ No

If yes, what PII elements are accessed, processed, or generated by the AI/ML component?

☐ Name/Former Name	☐ Date of Birth	☐ Maiden Name	☐ Place of Birth	☐ Citizenship
☐ Social Security number (including in truncated form)	☐ Driver's License	☐ Financial Account	☐ Taxpayer ID	☐ Passport Number
☐ Sex	☐ Telephone Number	☐ Criminal Record	☐ Education	☐ Age
☐ Financial Transaction	☐ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☐ Employee ID
☐ Credit Card	☐ Medical Record	☐ File/Case ID	☐ Financial Information	☐ Religion
☐ Alias	☐ Home Address	☐ Military Service	☐ Mother's Maiden Name	☐ Medical Information
☐ Email Address	☐ Marital Status	☐ Race/Ethnicity	☐ Occupation	☐ Work Email Address
☐ Job Title	☐ Salary	☐ Business Associates	☐ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☐ Work Address	☐ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☐ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☐ Weight	☐ Voice/Audio Recording	☐ Eye Color



☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☐ Height	☐ Retina/Iris Scans
☐ User ID	☐ IP Address			
			☐ Other PII.	

Does the AI component transmit/maintain PII to any external systems, vendors, or cloud services?

How is PII protected when used by the AI/ML component?



APPROVAL SIGNATURE PAGE

Reviewed by: Scott Ewalt, OIG Authorizing Officer (AO)

SCOTT EWALT Digitally signed by SCOTT EWALT
Date: 2026.08.24 10:33:26 -04'00'

Signature



THE FOLLOWING OFFICIALS HAVE REVIEWED THIS DOCUMENT

Reviewed by: Efua Colecraft, Information System Security Officer (ISSO)-OIG ☒

Reviewed by: Todd Bailey, Acting Chief Information Officer, OIG ☒

Reviewed by: Lisa Finnican, OIG Attorney Advisor ☒

Reviewed by: Muhammad Butt, Emerging Technology and Senior Advisor for Cybersecurity Initiatives OASAM-OCIO ☒

Reviewed by: Mara Blumenthal, DOL Privacy Office Branch Chief OASAM-OCIO ☒