



U.S. DEPARTMENT OF LABOR
Office of the Chief Information Officer

**OFFICE OF WORKERS' COMPENSATION
PROGRAMS'
OWCP WORKERS' COMPENSATION
SYSTEM (OWCS)
AND
OWCS CLOUD
PRIVACY IMPACT ASSESSMENTS**

VERSION 1.9

APRIL 2023

CONTROLLED

DOCUMENT REVIEW AND CHANGE HISTORY

Date	Filename / Version #	Revision Description	Author
11/13	1.0	Initial Version using OWCS	OWCP
10/14	1.1	Annual update	OWCP
11/15	1.2	Annual update	OWCP
11/16	1.3	Annual update	OWCP
11/17	1.4	Annual update	OWCP
11/18	1.5	Annual update	OWCP
2/20	1.6	Annual review and update	OWCP
3/20	1.61	Additional edits	OWCP
3/20	1.6	Record schedule information restated and updated for accuracy	OWCP BTS
3/21	1.7	Annual review and update.	OWCP/OCIO
4/22	1.8	Annual review and update.	OWCP/OCIO
3/23	1.9	Annual review and update.	OWCP/OCIO

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE	4
1.1. Overview.....	4
1.2. Characterization of the Information.....	6
1.3. Uses of the PII.....	12
1.4. Retention	14
1.5. Internal Sharing and Disclosure.....	17
1.6. External Sharing and Disclosure.....	18
1.7. Notice.....	21
1.8. Access, Redress, and Correction.....	25
1.9. Technical Access and Security	27
1.10. Technology	30
1.11. Determination	31
1.12. PIA Signature Page.....	32
 APPENDIX A: Definition For PII And PII Elements	 33

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1. OVERVIEW

In accordance with Department of Labor (DOL) guidelines the Office of Workers' Compensation Programs (OWCP) Division of Administration and Operations (DAO) and the Office of the Chief Information Officer (OCIO) conducted Privacy Impact Assessments (PIAs) on the OWCP Workers' Compensation System (OWCS) and OWCS Cloud systems.

OWCS is a multi-tenant major application IT framework that currently consists of six application components: The Energy Compensation System (ECS), DOL Site Exposure Matrix (DOL SEM), the OWCP Imaging System (OIS), the Correspondence Creation and Tracking System (CCAT), OWCP Connect, OWCP Landing Zone (LZ) Controller, and the E-Claimant Portal (which is a component of OIS, so not a separate component of OWCS):

- ECS provides a claims management system to support core business functions in administering the Energy Employees Occupational Illness Compensation Program Act (EEOICPA) of 2000 in support of the Division of Energy Employees Occupational Illness Compensation (DEEOIC).
- The DOL Site Exposure Matrix (DOL SEM) is a minor application of OWCS that supports ECS. It is a collection of three web portals with accompanying database information that allows DOL SEM users to support DEEOIC mission activities. DEEOIC staff use SEM as a tool to assist in evaluating exposure to toxic substances and causation for DEEOIC claims. DOL SEM does not contain any Personally Identifiable Information (PII).
- OIS provides imaging services to DEEOIC, the Division of Coal Mine Workers Compensation (DCMWC), and the Division of Longshore and Harbor Workers' Compensation (DFELHWC). The E-Claimant Portal is a component of OIS, which allows stakeholders to upload documents such as requests for informal conferences, forms, and medical reports to active OWCP cases. Users need an official OWCP case number and other identifying information to submit documents using the E-Claimant Portal. Once uploaded, the E-Claimant Portal assigns a unique document control number (DCN), which claimants can use to check the status of the document.

- CCAT currently provides a capability for OWCP's Program Offices to create and track various correspondence, such as letters, that are sent to claimants.
- OWCP Connect allows users to prove their identity and create an account for communication with OWCP's various self-service applications. It is a centralized identity-proofing system used to create credentials for a user, and then to authenticate the credentials for login. Identity proofing is accomplished by validating the user's information entered in the Account Registration process against secure Credit Bureau data. Once the user's identity has been verified, their account can be created. At this time OWCP Connect is only being used to authenticate new users to DFELHWC's Employees' Compensation Operations and Management Portal (ECOMP), as well as medical bill processing system users.
- The OWCP LZ Controller uses SSH encryption that comes included with the Secure File Transfer Protocol (SFTP) to securely transfer files to and from external vendors such as the medical bill and pharmacy benefits processing contractors.

OWCS Cloud consists of the following component:

- OWCS (Longshore) provides DFELHWC with case tracking and transaction history functionality on claims filed under the Longshore and Harbor Workers' Compensation Act (LHWCA) (and/or extensions). OWCS (Longshore) went into production in April 2020.

OWCP, in conjunction with OCIO, has determined that OWCS and OWCS Cloud process privacy information. As such, this document has been prepared to describe the information collected by OWCS and OWCS Cloud; what it is used for; who has access to the information; how the information can be corrected; and in general terms how the information is secured.

1.2. CHARACTERIZATION OF THE INFORMATION

OWCS and OWCS Cloud collect information on individuals or their survivors who claim benefits under the EEOICPA and the LHWCA (and/or extensions).

The EEOICPA covered individuals include but are not limited to employees or survivors of employees of the U.S. Department of Energy, its predecessor agencies, and their contractors and subcontractors. In addition to these individuals, the system contains information about attorneys representing claimants.

The LHWCA applies to employees injured or killed while working in private industry who are covered by the provisions of the LHWCA, the Non-Appropriated Fund Instrumentalities Act, the Defense Base Act, the Outer Continental Shelf Lands Act, referred to collectively herein as the LHWCA. In addition to these individuals, the system contains records of medical providers, insurance providers, attorneys and others representing claimants, rehabilitation counselors, and other health care professionals who provide information in support of compensation claims. Records are also kept on employers and insurance carriers who pay the benefits provided under this program.

The imaged documents for DEEOIC, DCMWC, and DFELHWC are documents provided in support of claims made under the EEOICPA, the Black Lung Benefits Act (BLBA), and the LHWCA. The BLBA provides monetary compensation and/or medical care to coal miners or qualified survivors of decedents who are totally disabled due to Pneumoconiosis (Black Lung) arising out of their employment in the nation's coal mines.

The E-Claimant Portal allows stakeholders to upload documents such as requests for informal conferences, forms, and medical reports to active OWCP cases.

CCAT currently provides a capability for DEEOIC to create and track various correspondence, such as letters, that are sent to claimants.

OWCP Connect allows users to prove their identity and create an account for communication with OWCP's various self-service applications.

LZ Controller allows file exchanges between OWCP and external contractors. These files involve items like eligibility, medical evidence, billing for pharmacy or medical, etc.

OWCS Cloud (aka OWCS (Longshore)) provides DFELHWC with case tracking and transaction history functionality on claims filed under the Longshore and Harbor Workers' Compensation Act (LHWCA) (and/or extensions).

- What are the sources of the PII in the information systems?

PII is provided to the agency in a variety of ways including:

- Forms submitted either by the individual claimant, their employer/agency their survivors or their employer insurance carrier or claim administrator. A list of the forms can be found at the following links:

https://www.dol.gov/owcp/energy/regs/compliance/claim_forms.htm

<http://www.dol.gov/owcp/dlhwc/lforms.htm>

<http://www.dol.gov/owcp/dcmwc/regs/compliance/blforms.htm>

- Reports by the employee
 - Reports by the U.S. Department of Energy
 - Reports by the Department of Health and Human Services
 - Reports by the Social Security Administration for earnings information
 - Reports from Insurance Companies
 - Employment records
 - Exposure records
 - Safety records or other incident reports
 - Dose reconstruction records
 - Workers' or family members contemporaneous diaries, journals, or other notes
 - Forms authorizing medical care and treatment
 - Other medical records and reports
 - Bills and other payment records
 - Compensation payment records
 - Formal orders for or against the payment of benefits
 - Transcripts of hearings conducted
 - Any other medical, employment, or personal information submitted or gathered in connection with the claim.
 - Communication between attorneys' representing claimants and the agency.
 - Other records of communication including notes on phone calls, letters, etc.
 - Documents submitted in support of claims for DEEOIC, DCMWC, and DFELHWC.
- What is the PII being collected, used, disseminated, or maintained?

- First and/or last name
 - Date of birth
 - SSN
 - Military, immigration, or other government-issued identifier
 - Residential address
 - Personal phone numbers (e.g., phone, fax, cell)
 - Mailing address (e.g., P.O. Box)
 - Medical information including physician's notes
 - Medical record number
 - Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
 - Financial Account Information and/or Numbers
 - Legal documents or notes (e.g., divorce decree, criminal records)
 - Employment History
 - Compensation Payment Data
 - Coordination of Benefits/Offset data
 - Survivor Eligibility Data, (e.g., relationship marriage, divorce, death)
 - Notes on debt collection/litigation issues
 - EEOICPA entitlement status
 - Medical bill information from the medical bill processing contractor – includes procedure codes, dates of service, and costs of service
 - Coded results of legal proceedings regarding claimant eligibility
 - Government Benefits data
 - Birth certificate
 - Marriage certificate
 - Death certificate
- How is the PII collected?
- PII is collected via paper forms which are then imaged in OIS and input into either the ECS, ASP, iFECS, or OWCS (Longshore) systems. (NOTE: For more information about iFECS and ASP please see their respective PIA documents.) Claimants may also upload their records directly into the system electronically.

For ECS the process is initiated with the receipt of a claim. The claim is reviewed to determine if it is covered under Part B or Part E of the EEOICPA. The requirements for eligibility are:

- Fact of Illness/Medical Evidence

- Fact of Covered Employment
- Fact of Exposure

A Claims Examiner (CE) reviews all the information submitted with the claim; however, he/she may need and obtain additional information to support the claim. The District Office CE or Senior CE issues a recommended decision. All recommended decisions are reviewed and finalized by the Final Adjudication Branch (FAB). If the claim is accepted, it is determined if the claimant will receive lump-sum payments and/or medical benefit payments.

The claimants may accept the recommended decision by waiving their rights to review or may dispute the decision by requesting a review of written record or an oral hearing before the FAB.

When a Final Decision has been made and payment is to be issued, the claimant is required to complete an acceptance of payment form and has the option to receive payments electronically transferred using the Electronic Funds Transfer (EFT) system or by paper check.

For OIS the documents are imaged and stored electronically for use by the respective systems.

For OWCS (Longshore), DFELHWC has a number of forms that are used to collect data in support of a claim. The majority of those forms are available on the Internet. These forms can be uploaded via SEAPortal (E-Claimant Portal), mailed, or faxed to DFELHWC.

Upon receipt of the Longshore forms, they are routed to the case if one exists. If a case does not exist a clerk creates a new case.

Medical reports and records are routinely submitted to DFELHWC as required by law. Claims staff may use OWCS (Longshore) to annotate medical diagnosis and other PII information.

- How will the information collected from individuals or derived from the systems be checked for accuracy?

For ECS: A claimant submits a claim for benefits and employment history forms to the District Office, Regional Resource Center (RRC) or the DEEOIC web site. Forms that are received at the RRC are sent to the District Office. After identifying the applicable part of the Act, a Case Create Clerk enters the form directly in the forms screen in ECS. When the information is entered it becomes a claim file. The Claims Examiner reviews the accuracy of the information that is entered by the Case Create Clerk, comparing the claim form to the information in ECS. If the information is not correct, certain elements

can be changed by the Claims Examiner, but other role-sensitive elements are returned to the Case Create Clerk for correction.

For OIS: Paper forms are reviewed and checked for accuracy by the responsible claims examiners and staff and the pertinent information is entered into the system. System edit checks help to ensure the accuracy of the data on the forms.

For the E-Claimant Portal: Forms are uploaded from the internet into OIS and reviewed and checked for accuracy by the responsible claims examiners and the pertinent information is entered into the system. System edit checks help to ensure the accuracy of the data on the forms.

For CCAT: Existing information is pulled from relevant databases and is checked for accuracy by the responsible claims examiners. CCAT does not create or collect new information.

For OWCP Connect: Identity proofing is accomplished by validating the user's information entered in the Account Registration process against secure Credit Bureau data. OWCP Connect does not create or collect new information.

For LZ Controller: Files are sent via secure, encrypted transmission and verified via SFTP+ native controls. Records sent are reviewed either by the contractor, OWCP or both.

For OWCS (Longshore), designated documents are reviewed and checked for accuracy by the responsible claims examiners and staff and the pertinent information is entered into the system. System edit checks help to ensure the accuracy of the data on the forms.

- What specific legal authorities, arrangements, and/or agreements allow the collection of PII?

For Energy: OWCP has been authorized by Congress (Public Law 106-398: National Defense Authorization Act for Fiscal Year 2001) to require persons who file notices of injury and/or claims for compensation under the Energy Employees Occupational Illness Compensation Program Act of 2000 and its extensions to disclose certain identifying information, including SSN. Consequently, applicable regulations, including 20 CFR 702.202 concerning the employer's report of an employee's injury or death, have been amended to expressly require the reporting of the injured worker's SSN. The amended regulations are contained in the Federal Register dated December 23, 1993 (58 FR 68032).

For Longshore: OWCP has been authorized by Congress (Public Law 103-112) to require persons who file notices of injury and/or claims for compensation under the Longshore and Harbor Workers' Compensation Act (LHWCA) and its extensions to disclose certain

identifying information, including SSN. Consequently, applicable regulations, including 20 CFR 702.202 concerning the employer's report of an employee's injury or death, have been amended to expressly require the reporting of the injured worker's SSN. The amended regulations are contained in the Federal Register dated December 23, 1993 (58 FR 68031).

For Black Lung: OWCP has been authorized by Congress (Public Law 92-303: The Black Lung Benefits Act of 1972) to require persons who file claims for compensation under the Black Lung Benefits Act of 1972 and its extensions to disclose certain identifying information, including SSN.

- Privacy Impact Analysis

There are many potential risks when medical information is recorded about an individual, such as identity theft, certain types of insurance coverage being refused if certain medical information became public, loss of employment, etc. The risk of PII being disclosed inadvertently when information is being passed between medical offices, other medical staff and OWCP is taken very seriously. OWCP understands its obligation to safeguard this information to prevent any of the potential risks from being realized and has established policies and procedures to safeguard this information. Throughout the remainder of this document examples of those safeguards have been explained to illustrate this commitment to prevention of PII being compromised.

In addition to the safeguards OWCP has in place internally, OWCP requires its medical and pharmacy bill payment contractors' operations to be in full compliance with Federal security guidance to ensure proper safeguards are in place to prevent the accidental release of information that has been entrusted to the organization.

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.

OWCP uses the collected PII as critical information for the purposes of managing the claimant's case and successfully fulfilling the mission. Imaged documents in OIS are used to support claims activities and are simply electronic copies of paper documents received by the respective program office responsible for the claim.

ECS operations provide the following functions which in some part depend on PII:

- Conduct correspondence with claimants, attorneys, and various medical personnel to determine the eligibility of the claim.
- Determine whether a claim is eligible or not and notify the claimant.
- Calculate the amount of benefits the claimant is eligible for.
- Receive electronic file of approved payments from the medical bill payment contractor's operation for transmission to the Treasury Department.
- Disburse benefit payments to claimants or their beneficiaries.
- Review pre-authorization requests for medical procedures.
- Conduct hearings and reviews when a claimant or his/her representative has filed an appeal.
- Provide statistics for quality reviews including utilization review and fraud and abuse detection.

DFELHWC uses the collected PII as critical information for the purposes of managing the claimant cases under the LHWCA.

OWCS (Longshore) operations provide the following functions which in some part depend on PII:

- Input and process claims.
- Conduct correspondence with claimants, attorneys, and various medical personnel to determine the eligibility of the claim.
- Determine whether a claim is eligible and notify the claimant.
- Periodically update claimant and medical information to determine continued eligibility.
- Calculate the amount of benefits the claimant is eligible for.

- In a limited number of cases, enter information to establish payment records for transmission to the Treasury Department.
- Support rehabilitation training and counseling.
- Resolve claim disputes between employees and employers and insurance carriers.
- Provide statistical data for program management.
- What types of tools are used to analyze data and what type of data may be produced?

For ECS and OWCS (Longshore) data mining is used to look for instances of potential fraud, as well as for reporting purposes, i.e. to determine if performance goals are being met. OIS simply provides imaging and storage of documents. The E-Claimant Portal is simply an external portal for OIS. CCAT is a correspondence creation and tracking system. OWCP Connect allows users to prove their identity and create an account for communication with OWCP's various self-service applications. LZ Controller provides a secure Landing Zone for file exchanges.

- Will the systems derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

No.

- If the systems use commercial or publicly available data, please explain why and how it is used.

The systems do not.

- Privacy Impact Analysis

All systems' users are required to read and sign the Rules of Behavior before being granted access to the system and review these annually. OWCS and OWCS Cloud use least privilege principles to ensure that only those who need access to the data to fulfill the agency's mission are given access in addition to the authentication controls discussed above.

The systems maintain only PII that is necessary and relevant to accomplish the purpose for which it is being collected.

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?

DFELHWC Record Control Schedule DAA-0271-2017-0005 “Division of Longshore and Harbor Workers’ Compensation” denotes that claim records are temporary and scheduled to be destroyed when no longer needed.

DEEOIC Record Control Schedule DAA-0271-2017-0006 “Division of Energy’s Employee’s Occupational Illness Compensation Records” denotes that claim records are temporary and scheduled to be destroyed 20 years after the program has been discontinued.

DCMWC Record Control Schedule DAA-0271-2017-0004, “Division of Coal Mineworkers’ Compensation (DCMWC)” denotes that the majority of claims data is temporary and scheduled to be destroyed after a period of 10-50 years after cutoff depending on the data. Part of the DCMWC data is considered to be permanent and is transferred to NARA 15 years after cutoff.

- Is a retention period established to minimize privacy risk?

Yes. NARA approved Record Control Schedules DAA-0271-2017-0005, DAA-0271-2017-0006, DAA-0271-2017-0004, and DAA-0271-2017-0003.

- Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes

- How is it determined that PII is no longer required?

The OWCP programs, under which PII records are collected and processed, are authorized by Congress to collect such information. Because these records are part of the official record that justifies the compensation decisions made by OWCP, they are required to be maintained as part of the audit record for the agency until such time as they are destroyed per NARA and DOL guidelines.

- Per M-O7-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the systems if it is no longer required?

OWCP collects only the PII necessary to process claims under its statutory authority. Paper records are being replaced by electronic files which are dispositioned according to RCS temporary parameters.

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

Yes, OWCP has a clause in all of its MOUs, which states that all PII extracts will be deleted within 90 days of the date that the data was extracted.

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

OWCP follows all NIST 800-53 Rev. 5 requirements for the safeguarding of PII. OWCP removes all sensitive PII from data extracts such as the full SSN and only includes a minimum amount of PII in external correspondence in order to minimize the potential for a PII breach. OWCP also encrypts email attachments and external media that contain PII. All reports from the systems contain only the minimum required amount of information to avoid PII compromise.

- Privacy Impact Analysis

OWCS and OWCS Cloud contain data on all four of OWCP's programs. This data is maintained on secure servers that are regularly scanned to prevent intrusion. OWCP has implemented new NARA retention schedules.

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?

Electronic case records can be requested by the following organizations outside of the OWCP program for auditing purposes: the DOL Office of Inspector General (OIG) and the Office of the Chief Financial Officer (OCFO) for audit purposes; and the Office of the Solicitor (SOL) for litigation support.

- How is the PII transmitted or disclosed?

“Read only” access to data is provided to auditor user accounts for temporary periods required by the auditors. If any PII has to be transmitted to an auditor, it is done through an encrypted E-Mail attachment, password protected E-Mail attachment, or via an approved portal specifically designed for the secure upload of audit-related documents.

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

Yes, OWCP has a clause in each of its MOUs relating to data sharing that stipulates a requirement to review the MOU on an annual basis to ensure that the requirement to share information is still valid.

- Privacy Impact Analysis

The sharing of data with internal users is limited to SOL for litigation support; and the OIG and OCFO and their designated auditors. All auditors are required to sign strict non-disclosure agreements, read and sign Rules of Behavior and complete security screening before they are authorized to access any data. The information is being shared with auditors and the SOL for civil or criminal law enforcement.

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?

The following agency receives ECS and OWCS (Longshore) data via Connect:Direct.

- Department of the Treasury – Fiscal Service (FS) - disposition of OWCS benefit payments to and on behalf of beneficiaries

Harper, Rains, Knight & Company receives Longshore data by CD. The Longshore data is used by the company to audit Longshore insurance carriers on behalf of OWCP to ensure claims are being reported timely and accurately.

Data is shared with the Energy Program's contract resource centers that have read-only access to OIS. Data is also shared with the Department of Energy (DOE), the Social Security Administration (SSA), the Department of Health and Human Services, as well as with contracted industrial hygienists.

As stated earlier, DEEOIC receives documents from its medical bill processing contractor for purposes of prior authorization and other claims management. Also, as part of its contract with OWCP, the medical bill processing contractor prepares files for transmission to the U.S. Treasury for payments to be made. These payments are authorized and approved by the OWCP program office, so no transaction is completed without the intervention of authorized federal staff who confirm the payments.

E-Claimant Portal, CCAT, and OWCS (Longshore) have no external connections. OWCP Connect receives data from a third party in order to validate identity. OIS receives files from insurance carriers and the central mail room through a landing zone on the General Support System.

- 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.

Yes. It is covered by DOL/OWCP-11 and DOL/OWCP-3. Authorization is granted via a Memorandum of Understanding (MOU) and/or an Interconnectivity Security Agreement (ISA) between OWCP and the outside Agencies.

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

The transmission of data is done through a direct connection which includes two factor authentication and encryption of the data. The information is also shared via portable media (CD) and is encrypted with the DOL mandated encryption software.

- How is the information transmitted or disclosed?

The transmission of data is done through a direct connection, which includes two factor authentication and encryption of the data. The information is also shared via portable media (CD) and is encrypted with the DOL mandated encryption software.

- 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 yes, include who the agreement is with and the duration of the agreement.

Yes. OWCP has MOUs with the Department of the Treasury and Harper, Rains, Knight & Company, which reflect the scope of the information currently shared and is reviewed annually and re-signed every five years.

OWCP has a contract and an MOU in place with its medical and pharmacy bill processing contractors. The contracts reflect the scope of the information currently shared and the requirements to protect that information.

- How is the shared information secured by the recipient?

All of OWCP's MOUs and contracts state that all shared information shall be secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

All of OWCP's MOUs and contracts state that annual Privacy Act and Information Security Awareness training shall be conducted for all employees who have access to the shared information.

- Privacy Impact Analysis

The external sharing of data is the required connections to the medical and pharmacy bill processing contractors' operations and the Treasury's FS.

Since the connection is made through the DOL network, an Interconnection Service Agreement is in place between DOL and Treasury's FS. In addition, an MOU between the DOL and U.S. Treasury Department is also in place covering this connection. The data is used in order for checks to be issued to claimants.

There are also security provisions as part of the contract in place between OWCP and the medical and pharmacy bill processing contractors' operations to cover these connections.

The external sharing of Longshore data is required for DFELHWC and Harper, Rains, Knight & Company to ensure claims are being reported timely and accurately.

An MOU between OWCP and Harper, Rains, Knight & Company is also in place covering this data exchange by CD. As indicated above, the CD is encrypted before being sent to guard against unauthorized use in the event the CD is misdirected.

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. 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.

Privacy Act considerations are included on the back of our claimant forms. Claimants are instructed to review the entire document before submitting the form.

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

Yes, we have the following statements included in our claimant forms:

For DEEOIC:

In accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a), you are hereby notified that:

(1) The Energy Employees Occupational Illness Compensation Program Act (42 U.S.C. 7384 et seq.) (EEOICPA) is administered by the Office of Workers' Compensation Programs of the U.S. Department of Labor, which receives and maintains personal information on claimants and their immediate families.

(2) Information which the Office has received will be used to determine eligibility for, and the amount of, benefits payable under EEOICPA, and may be verified through computer matches or other appropriate means.

(3) Information may be given to the Federal agencies or private entities that employed the claimant at the time of injury in order to verify statements made, answer questions concerning the status of the claim, verify billing, and to consider other relevant matters.

(4) Information may be disclosed to physicians and other health care providers for use in providing treatment, making evaluations for the Office of Workers' Compensation Programs and for other purposes related to the medical management of the claim.

(5) Information may be given to Federal, state, and local agencies for law enforcement purposes, to obtain information relevant to a decision under the EEOICPA, to determine whether benefits are being paid properly, including whether prohibited payments have been made, and, where appropriate, to pursue salary/administrative offset and debt collection actions required or permitted by the Debt Collection Act.

(6) Disclosure of the claimant's social security number (SSN) or tax identification number (TIN) is mandatory. The SSN or TIN, and other information maintained by the Office, may be used for identification, to support debt collection efforts carried on by the Federal government, and for other purposes required or authorized by law.

(7) Failure to disclose all requested information may delay the processing of the claim or the payment of benefits, or may result in an unfavorable decision.

For Longshore:

In accordance with the Privacy Act of 1974, as amended, 5 U.S.C. 522a), you are hereby notified that:

- (1) The Longshore and Harbor Workers' Compensation Act, as amended and extended (33 U.S.C. 901 et seq.) (LHWCA) is administered by the Office of Workers' Compensation Programs of the U.S. Department of Labor which receives and maintains personal information on claimants and their immediate families;
- (2) Information which the Office has will be used to determine eligibility for the amount of benefits under the LHWCA;
- (3) Information may be given to the employer which employed the claimant at the time of injury, or to the insurance carrier or other entity which secured the employer's compensation liability;
- (4) Information may be given to the physicians and other medical service providers for use in providing treatment or medical/vocational rehabilitation, making evaluations and for other purposes relating to the medical management of the claim;
- (5) Information may be given to the Department of Labor's Office of Administrative Law Judges (OALJ), or other person, board or organization, which is authorized or required to render decisions with respect to the claim or other matter arising in connection with the claim;
- (6) Information may be given to Federal, state and local agencies for law enforcement purposes, to obtain information relevant to a decision under the LHWCA, to determine whether benefits are being and have been paid properly, and, where appropriate, to pursue salary/administrative offset and debt collection actions required or permitted by law;
- (7) Disclosure of the claimant's SSN or tax identifying number (TIN) on this form is mandatory. The SSN and/or other information maintained by the Office may be used for identification, and other purposes authorized by law;
- (8) Failure to disclose all requested information may delay the processing of the claim, the payment of benefits, or may result in an unfavorable decision or reduced level of benefits.

For DCMWC:

In accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a) you are hereby notified that

- (1) the Black Lung Benefits Act (BLBA) (30 U.S.C. 901 et. seq.) as amended, is administered by the Office of Workers' Compensation Programs (OWCP) of the U.S. Department of Labor, which receives and maintains personal information, relative to this application, or claimants and their immediate families.

(2) information obtained by OWCP will be used to determine eligibility for the amount of benefits payable under the BLBA;

(3) information may be given to coal mine operators potentially liable for payment of the claim, or to the insurance carrier or other entity which secured the operator's compensation liability;

(4) information may be given to the physicians or medical service providers for use in providing treatment, making evaluations and for other purposes relating to the medical management of the claim;

(5) information may be given to the Department of Labor's Office of Administrative Law Judges, or other person, board or organization, which is authorized or required to render decisions

with respect to the claim or other matters arising in connection with the claim;

(6) information may be given to Federal, state or local agencies for law enforcement purposes, to obtain information relevant to a decision under the BLBA, to determine whether benefits are being or have been paid properly, and, where appropriate, to pursue administrative offset and/or debt collection actions required or permitted by law;

(7) disclosure of the claimant's Social Security Number (SSN) or tax identifying number (TIN) on this form is voluntary. The SSN and/or TIN and other information maintained by the OWCP may be used for identification and for other purposes authorized by law;

(8) failure to disclose all requested information may delay the processing of this claim or the payment of benefits or may result in an unfavorable decision or a reduced level of benefits.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

As indicated in the previous question, OWCP has been authorized by law to collect certain information in order to process claims. The information is used only for the purposes of managing the claim. Claimants consent to this use of their information by signing the claimant form.

- Privacy Impact Analysis

Specific notice of the need to have and use privacy data to process a claim is included on the claim form itself to ensure that all claimants are aware of the data necessary to complete their claim and its uses. In addition, System of Records Notices (SORNs) which outline the users of privacy data for this system are available to the public through the DOL internet. (See reference of SORN in Section 1.6 above)

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?

Claimants have the right to request a copy of their files at any time.

- What are the procedures for correcting inaccurate or erroneous information?

For ECS: Claimants can contact the closest OWCP-DEEOIC or RRC office and provide amended information. They are also periodically contacted by DEEOIC claims administrators to request updated information for their claim as needed to adjudicate the claim.

For OWCS (Longshore), claimants can contact DFELHWC and provide amended information.

For OIS, CCAT, and E-Claimant Portal: Claimants may provide amended documents if there is something inaccurate or missing from a document provided. This would be handled by the respective program office's claims staff. For OWCP Connect, OWCP receives validation acknowledgments from a third party credit bureau and is not responsible for the accuracy of the data received.

For LZ Controller: If the files transmission fails or a corrupted file is received, the file is resent.

- How are individuals notified of the procedures for correcting their own information?

At the time they file the claim they are informed that they should contact the office should there be any changes in the information provided. OWCP is also in regular communication with the claimant providing the opportunity for correction of information throughout the life of the claim.

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

Individuals have access, redress, and amendment rights under the Privacy Act for their records, and the procedures pertaining thereto are documented in the Privacy Act system of records notice.

- Privacy Impact Analysis

Electronic access to the claimant's records is strictly limited to preserve the privacy of the claimant. Only the claimants and their legal representatives have the right to a copy of the administration claim file and can request copies of their records to avoid any potential breach of privacy.

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.)

For ECS, OIS, and CCAT: Claims Examiners, District Directors, Fiscal Officers, Field Nurses, Policy Program Analysts, Deputy Director, Director, and Branch Chiefs have access to the system based on their individual roles. A few software developers, and testers, as well as the Energy Program Resource Centers, have limited access to the system. Two Help Desk Staff, one developer lead, and one Application Project Manager have write access to ECS to perform certain duties.

For OWCS (Longshore): Administrators, Directors, Policy Chiefs, Policy Examiners, Fiscal Chiefs, Fiscal Examiners, Program Analysts, District Directors, Claims' Examiners, Claims' Assistants, Case Create Supervisors, Case Create Clerks, and Auditors have access to the system based on these individual roles. There is also a handful of contractors who have production access to the system as follows: four Administrators and four Program Analysts.

There is no public access to any of these systems, other than to submit information through the E-Claimant Portal.

- Do the systems use "roles" to assign privileges to users of the system? If yes, describe the roles.

Yes, the systems use roles to assign privileges to users of the system.

For ECS: The roles include various levels of Claims Examiners (including Supervisory Claims Examiners, Claims Managers, etc.), Case Create Clerks, Fiscal Officers, Field Nurses, District Directors, Resource Center employees, and read-only access roles assigned to people like testers, and developers. Furthermore, write access to ECS is granted to two Help Desk staff, one developer lead, and one Project Manager.

For OWCS (Longshore): The roles include the following: Administrators, Directors, Policy Chiefs, Policy Examiners, Fiscal Chiefs, Fiscal Examiners, Program Analysts, District Directors, Claims' Examiners, Claims' Assistants, Case Create Supervisors, Case Create Clerks, and Auditors. There is also a handful of contractors who have production access to the system as follows: four Administrators and four Program Analysts.

- What procedures are in place to determine which users may access the systems and are they documented?

OWCP and OCIO have put in place access control measures that include documented user access authorizations, encryption and least privilege. Detailed access control, as well as other security control information is recorded in the OWCS and OWCS Cloud System Security Plans.

- Will Department contractors have access to the systems? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA.

OWCP contractors are required to read the Information System Security and Privacy Awareness Training slides and the OWCP MA Rules of Behavior and sign a Non-Disclosure Agreement before accessing the system. Also a Personal Identity Verification (PIV) is conducted on each contractor.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?

Annual Information System Security and Privacy Awareness Training, which has a privacy module or component to it.

- What auditing measures and technical safeguards are in place to prevent misuse of data?

OWCS and OWCS Cloud use the concept of least privilege as described above. Access is granted only after authorization based on documented access request policies. Logs for certain system functions are also reviewed on a regular basis to check for any misuse or other issues.

All OWCP operations are required to have security audits and assessments conducted of their operations on an annual basis. All OWCP systems must have system level auditing enabled to provide for reasonable response in the event of a security situation. IT system auditing and security testing is an essential aspect of how the Agency ensures the integrity and availability of our computing systems. Auditing and assessments also provide the Agency the ability to be more effective in preventing security vulnerabilities.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

Yes, the data is secured in accordance with FISMA requirements. An Annual Security Assessment (ASA) for OWCS, as part of an on-going authorization, was last completed on 01/04/2023. An ASA for OWCS Cloud, as part of an on-going authorization, was last completed on 3/22/2023. An ASA is performed every year on all systems.

- Privacy Impact Analysis

There are many potential risks when medical information is recorded about an individual, such as identity theft, certain types of insurance coverage being refused if certain medical information became public, loss of employment, etc. OWCP understands its obligation to safeguard this information to prevent any of the potential risks from being realized. Throughout this document examples of those safeguards have been explained to illustrate this commitment to prevention of PII being compromised.

There are appropriate administrative, technical, and physical safeguards in place to ensure the security and confidentiality of the 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.

- Were the systems built from the ground up or purchased and installed?

The systems were all built from the ground up.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your systems.

Considerations regarding data integrity, privacy, and security were analyzed and included in all system development life cycle phases.

- What design choices were made to enhance privacy?

OWCP designed the system around the concepts of least privilege and separation of duties. This is implemented through the use of various roles that have access only to the information that is required to perform a particular role. OCIO also implemented several IT controls (such as a firewall, IDS, IPS, etc.) in order to prohibit unauthorized access from external parties.

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

OWCS and OWCS Cloud components are all in the Operations and Maintenance phase.

The DOL System Development Life Cycle Management (SDLCM) Manual.

- Does the project employ technology which 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?

OWCP has completed the PIA for OWCS and OWCS Cloud which are currently in operation. OWCP has determined that the safeguards and controls for this moderate system adequately protect the information.

OWCP 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

Signature of OWCS System Owner

Robin Crisp
Print Name

Signature of OWCS Cloud System Owner

Alain Cimon
Print Name

APPENDIX A: DEFINITION FOR PII AND PII ELEMENTS

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, or ☒ Members of the Public. {Check all that apply}

- ☒ First and/or last name
- ☒ 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: Employment History
 - ☒ Other: Compensation Payment Records
 - ☒ Other: Coordination of Benefits/Offset data
 - ☒ Other: Survivor Eligibility Data, (e.g., relationship marriage, divorce, death)
 - ☒ Other: Notes concerning debt collection/litigation issues
 - ☒ Other: Medical Condition Status
 - ☒ Other: EEOICPA entitlement status
- Is any part of the PII collection voluntary?

All PII collection is voluntary in the sense that no one is forced to provide any personal information. However, the refusal to provide the requested information may result in a denial of the claim for benefits.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

OWCP follows all NIST 800-53 Rev. 5 requirements for the safeguarding of PII. OWCP removes all sensitive PII from data extracts such as the full SSN and only includes a

minimum amount of PII in external correspondence in order to minimize the potential for a PII breach. OWCP also encrypts email attachments and external media that contain PII. All reports from the systems contain only the minimum required amount of information to avoid PII compromise