PRIVACY IMPACT ASSESSMENT

Effective Date: Month Day, Year

Office of Workers' Compensation Programs (OWCP) Energy Program Systems

☒ Concurrence of Senior Agency Official for Privacy

☐ Non-concurrence of Senior Agency Official for Privacy

Carolyn Angus-Hornbuckle

Digitally signed by Carolyn Angus-Hornbuckle
Date: 2024.10.11 17:04:13 -04'00'

Carolyn Angus-Hornbuckle, SAOP

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, OWCP 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)

OWCP's Energy Program and the systems it operates, including components of the Office of Workers Compensation System (OWCS) and the Employees' Compensation Operations and Management Portal (ECOMP).

Location of the System

OWCS and ECOMP are hosted on the DOL General Support System (DOL GSS) Amazon Web Services (AWS) Cloud instance. The OWCS security boundary consists of six applications: Energy Compensation System (ECS), OWCP Imaging System (OIS), Correspondence Creation and Tracking System (CCAT), OWCP Connect, E-Claimant Portal (which is considered part of OIS, so is not a separate application), the OWCP Landing Zone (LZ) Controller, and the DOL Site Exposure Matrix (DOL SEM site). The Energy Program has approximately 500 users who are in OWCP Offices and telework locations throughout the continental U.S. The Energy Program's primary claims' processing application (ECS) is only accessible to internal DOL users following successful login to the DOL GSS network via a Personal Identity Verification (PIV) card.

Brief Description of the System

Although this PIA is specific to the OWCP's Energy Program, OWCS supports three compensation programs that provide wage replacement benefits, medical treatment, vocational rehabilitation and other benefits to certain workers or their dependents who experience work-related injury or occupational disease, as follows:

- the Energy Employees Occupational Illness Compensation Program,
- the Longshore and Harbor Workers' Compensation Program, and
- the Black Lung Benefits Program.

OWCS is a security boundary that currently consists of six application components:

- The Energy Compensation System (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 sub-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) and is categorized as a Federal Information Processing Standards (FIPS) 199 Low system.
- The OWCP Imaging System (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 further sub-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.
- The Correspondence Creation and Tracking System (CCAT) currently provides a capability for the Energy Program 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 OWCP's Employees' Compensation Operations and Management Portal (ECOMP), the Federal Employees' Compensation Act's (FECA) Pharmacy Benefits Manager (PBM), as well as medical bill processing system users.
- The OWCP Landing Zone (LZ) Controller uses Secure Shell (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.

ECOMP is a component of the Integrated Federal Employees' Compensation System (iFECS). ECOMP provides a portal for claimants and their authorized representatives to review claims' status.

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: Demographic information is collected to improve program accessibility and inclusion in support of program administration.

This System is operated by:

☒ Component agency: Office of Workers' Compensation Programs (OWCP)

☐ Contractor

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

☐ Yes
☐ No

Provide explanation if No is checked.

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 3-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. The President's Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government provides authority for collection of demographic data not previously collected by OWCP.

☐ Changed business processes. Insert explanation.

☐ 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, financial, or demographic information).

☐ Other: **Specify.**

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

☒ General Public (individual claimants, which includes authorized representatives, have access only to their own data in the information system as it relates to their claim for benefits or in connection with the other self-service parts of the system).
☒ Contractors
☒ Government Employees
☐ Other: Click or tap here to enter text.

1. INFORMATION IN THE SYSTEM

OWCP 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
☐ Maiden Name
☐ Citizenship
☒ Date of Birth
☐ Place of Birth

☒ Social Security number (including in truncated form)
☐ Driver's License/Other Government ID
☒ Financial Account
☐ Taxpayer ID
☐ Passport Number
☒ Gender or Gender Identity
☒ 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: Legal documents or notes, birth certificates, marriage certificates, death certificates, government benefits data, disability status, primary language, notes on debt collection/litigation issues, survivor eligibility data

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: Claimants can designate authorized reps to file claims for them.
☐ Other: Specify.		

Government Sources		
☐ Within the Component Agency	☐ Other DOL component agencies	☒ Other Federal Agencies
☐ State, Local, Tribal	☐ Foreign	☐ Other: Specify.

Non-government Sources		
☒ Public Organizations	☐ Private Sector	☐ Commercial Data Brokers
☐ Third Party Website or Application		☒ Other: Medical service providers, medical and pharmacy bill processing contractors

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, regulation, 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?

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.

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

SSN is used to ensure benefit payments are made to the correct person.

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

Case/claim number.

1.4.4. The alternatives were not selected because:

Case/claim number are used extensively in the system; however, these are not able to establish an absolute unique identifier to ensure payments are properly disbursed.

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 that does not currently have an OMB control number is the Voluntary Demographic Collection for Energy and Coal Miners.
- ☒ The information collected is part of an existing collection and the OMB control number for the collection is: 1240-0002, 1240-0044, 1240-0007, 1240-0019, 1240-0037, 1510-0007, 1240-0060,

☐ 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 Energy Program's mission, under the Energy Employees Occupational Illness Compensation Program Act (EEOICPA), is to protect the interests of workers who were injured or became ill on the job, or their families, by making timely, appropriate, and accurate decisions on claims and providing prompt payment of benefits to eligible claimants.

The Energy Program also intends to collect voluntary demographic information for Energy claimants. Demographic information is collected to improve program accessibility and inclusion, including with respect to overall outcomes.

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:

Energy Employees Occupational Illness Compensation Program Act of 2000, Title XXXVI of Pub. L. 106-398, October 30, 2000, 114 Stat. 1654, and as amended.).

E.O. 13985 - Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, January 20, 2021; and E.O. 14091 - Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, February 16, 2023.

3. INTENDED USE OF THE INFORMATION

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

Energy Program uses the information for the following purposes:

- Conduct correspondence with claimants, authorized representatives, 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 U.S. Department of the Treasury.
- 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.
- Report on the Energy Program's status to Congress.
- Analyze the voluntary demographic information to ensure determine if the Program needs to improve equity, accessibility, and inclusion in getting information out to the public and in the processing of claims.

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

☒ Yes: The ECS application uses data mining 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.

The data from the voluntary demographics form is stored in OIS – not ECS – so is stored separately from the claims processing system. The forms will be stored under a dedicated tab in OIS and will not be stored within the case. The forms can be linked to a particular case in OIS, but will not be viewable by CEs, Supervisors, or others without proper "permissions" to view the documents. The only reason they will be linked to the case is to provide the claimant the ability to re-submit updated voluntary demographics data. These forms will not be part of any claimant's claims for benefits. The data will be manually analyzed by only a few OWCP management analysts to look for trends that can allow for OWCP to improve customer experience. The voluntary demographics forms can be submitted via mail or via the E-Claimant Portal. OWCP may use spreadsheets and/or databases to assist in data analysis, but at this time no automated tools are in use.

☐ No

4. INFORMATION SHARING AND ACCESS

4.1. Will OWCP 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**
Office of the Inspector General	Any relevant case records pertaining to the audit.	Audit purposes.
Office of the Chief Financial Officer	Any relevant case records pertaining to the audit.	Audit purposes.
Office of the Solicitor	Any relevant case records pertaining to a particular issue being litigated.	Litigation support.

External Sharing			
Organization	**Information Shared**	**Purpose**	**MOU or other Agreement**
Department of the Treasury	Payment files	Pay benefits to claimants	MOU/ISA
OWCP's Medical Bill Processing Contractor (Acentra Health)	Processed medical bill and eligibility files.	Determine eligibility and process medical bills	MOU/ISA

Department of Health and Human Services/National Institute of Occupational Safety and Health (NIOSH)	Radiation exposure information	Determine eligibility for benefits, as well as amount and type of benefits.	MOU
OWCP Connect Third-Party Identity Validator (TransUnion)	Identity verification pass and fails	Remote identity verification of ECOMP and medical bill portal users.	Contract
OWCP's Pharmacy Bill Processing Contractor (Conduent)	Processed pharmacy bills and eligibility files.	Determine eligibility and process pharmacy bills.	Contract
Department of Energy	Nuclear weapons manufacturer facilities and information, including employment records.	Determine eligibility for benefits, as well as amount and type of benefits.	MOU

4.2. Does OWCP 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.
Entities receiving the data are required to notify OWCP before they can disseminate it.

☐ No, another DOL component agency is not required to verify with the component agency operating the system before re-dissemination of PII.
Explain here.

☐ 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.
All MOUs, ISAs, and contracts stipulate that the data is owned by OWCP and must not be disseminated without OWCP's consent.

☐ No, the external agency or entity is not required to verify with the DOL component agency before re-dissemination of PII.
Explain here.

☐ 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.

"Read only" access to data is provided to auditor user accounts for temporary periods required by the auditors. PII is usually redacted from any files sent to the auditors. However, if it is necessary to transmit any PII 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.

The Department of the Treasury receives ECS payment files via Connect:Direct in connection with disposition of Energy Program benefit payments to and on behalf of beneficiaries. IBM® Sterling Connect:Direct provides security-hardened, point-to-point file transfers to lessen dependency on unreliable File Transfer Protocol (FTP) transfers. It is optimized for high-volume delivery of files within and among enterprises. The solution ensures more reliable movement of files, from batch integration and movement of large images or catalogs, to synchronization with remote locations.

The medical and pharmacy bill processing files are exchanged via the OWCP LZ Controller. The OWCP LZ Controller sends files to a DOL-owned Secure File Transfer Protocol (SFTP) server, which uses Secure Shell (SSH) encryption that comes included with the SFTP to securely transfer files.

Files are transmitted between the Energy Program and HHS/NIOSH utilizing the Centers for Disease Control's secure CITRIX Storefront portal.

Files are transmitted between the Energy Program and DOE utilizing the DOE Secure Electronic Record Transfer (SERT) system, which is a secure web-based application.

☐ No, this system does not connect with or receive information from another system(s) authorized to process PII.

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:

Energy's forms can be found at:
https://www.dol.gov/owcp/energy/regs/compliance/claim_forms.htm

☐ Notice is provided by other means.
Specify how.

☒ 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.

Each form noted above has a Privacy Act Statement which indicates individuals may decline to provide information. However, failure to provide certain information may impact the ability of OWCP to process a claim successfully.

The demographic information is completely voluntary. The Privacy Act Statement on the demographic form will specifically note that providing some or all information is optional and that failure to provide information will not have an impact on a claim.

☐ No, individuals do not have an opportunity to decline to provide PII.
Specify why.

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.
Specify how.

☒ No, individuals do not have an opportunity to consent to particular uses of their PII.

Claimants consent to the use of their information by signing the claimant form. In connection with the Privacy Act Statements included on OWCP forms, individuals are consenting to the Routine Uses identified in the applicable SORN when they provide information. Although providing information to OWCP is generally not considered mandatory, certain claims-related information is needed to successfully reach a favorable decision regarding a claim. Additionally, the Privacy Act permits an individual to request their own records and give consent for another person to access their records.

The Energy Program may also collect voluntary demographic information about claimants. Demographic information is collected to improve program accessibility and inclusion and is provided on a strictly voluntary basis. Information will not be shared beyond the Routine Uses without consent as required under the Privacy Act of 1974. The claimants can choose not to provide certain demographic information by not filling out part or all of the form.

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.

Individuals who have records in the identified System of Records have the rights provided by the Privacy Act of 1974 and further explained in the System of Records Notice. In addition to the rights as outlined in the Privacy Act and SORN, users can contact the Energy Program and provide amended information to the forms they submitted at any time.

☐ No, individuals do not have an opportunity to review or update PII pertaining to them.
Specify why.

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.
Describe the safeguards in place for the physical location.

☒ All users signed a confidentiality agreement or non-disclosure agreement.

Only contractors are subject to the DOL Non-Disclosure Agreement (NDA).

☒ All users are subject to a Code of Conduct that includes the requirement for confidentiality.

Annual Cybersecurity & Privacy Awareness includes the DOL IT Rules of Conduct.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **annual** training on privacy and confidentiality policies and practices.

Annual Cybersecurity & Privacy Awareness Training

☒ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices.

All DOL employees and contractors receive Annual Cybersecurity & Privacy Awareness training. All Energy Program claims' examiners (CEs) and other claims' processing staff receive privacy-related training as part of their CE training program. Although claimants will be specifically instructed to not upload the voluntary demographic form to their case file via the portal, all Energy Program claims' processing staff will receive training on how to remove voluntary demographic forms if they come across any that have been uploaded by mistake to the case file by a claimant.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **system-specific** training on privacy and confidentiality policies and practices.

All DOL employees and contractors receive Annual Cybersecurity & Privacy Awareness training. All Energy Program claims' examiners (CEs) and other claims' processing staff receive privacy-related training as part of their CE training program. Although claimants will be specifically instructed to not upload the voluntary demographic form to their case file via the portal, all Energy Program claims' processing staff will receive training on how to remove voluntary demographic forms if they come across any that have been uploaded by mistake to the case file by a claimant.

☒ Access to the PII is restricted to authorized personnel only.

Only users authorized by the System Owner or designee are allowed access to the system.

☐ Appropriate NIST SP 800-53 Revision 4 security controls for protecting PII are imposed.
Please note if the controls were imposed through the ATO process and/or continuous monitoring such as a Security Assessment Report through an annual security assessment.

- ☐ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.
  Identify the last date the SAR was performed, the frequency of review of the SAR, and whether there were any controls imposed on the system that were found to not be implemented.

☒ Appropriate NIST SP 800-53 Revision 5 security controls for protecting PII are imposed.

Controls were imposed and tested as part of the DOL Security Control Assessment Plan (SCAP), which is part of the DOL's Continuous Monitoring Process.

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

An Annual Security Assessment (ASA) was last completed on 2/26/2024.

☐ There is one or more Plan of Action and Milestones (POA&M) associated with this system.

N/A – There are currently no open POA&Ms associated with OWCS.

☒ Contractors that have access to the system are subject to information security provisions in their contracts required by DOL policy.

All contracts have a privacy section that states that following: "Portions of information disclosed during the performance of this task are protected by the provisions of the Privacy Act of 1974; therefore, all personnel assigned to this Contract are required to take proper precautions to protect the information from disclosure. Additionally, all personnel assigned to this Contract must take an online training course for handling PII. This course is required before system access is granted and then must be completed annually by all employees with access to DOL systems."

☐ Contracts with customers establish DOL ownership rights over data including PII.

N/A – there are no contracts with customers.

☐ Other: Specify.
Describe.

6.2. Technological controls for the system:

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

Audit logs are reviewed monthly to ensure that only authorized individuals have access to the system.

☒ User Log In Credentials

To access OWCS's ECS, OIS, and CCAT components, a PIV card is required to access the network before access to the system is granted. Single Sign On (SSO) – with multi-factor authentication (MFA) – has been implemented for all OWCS internal-facing components. Access to ECOMP requires MFA

following successful ID proofing via OWCP Connect. The E-Claimant Portal does not have accounts associated with it because it only involves a one-way delivery of information – like mailing a letter.

☒ Virtual Private Network (VPN)

For OWCS, all remote users use a VPN (Zscaler) to access the DOL network before gaining access to OWCS internal-facing components via SSO/MFA. E-Claimant Portal, OWCP Connect, and ECOMP are accessible via the internet, so a VPN is not required.

☐ Biometrics
Describe any biometrics used to access the system, such as fingerprint, facial recognition, etc.

☒ Encryption of Data at Rest
All OWCS components are hosted on the DOL GSS Amazon Web Services (AWS) Cloud instance. AWS automatically encrypts data-at-rest.

☒ Firewall
The DOL GSS employs a firewall to protect the DOL network and systems hosted on the DOL network.

☒ Role-based Access Controls

OWCS's ECS, CCAT, and OIS components, as well as ECOMP, have roles that enable role-based access. The roles include various levels of Claims Examiners (including Supervisory Claims Examiners, Claims Managers, etc.), District Directors, Fiscal Officers, Field Nurses, Policy Program Analysts, Deputy Director, Director, and Branch Chiefs.

☒ Encryption of Data in Transit

SFTP and HTTPS are used to encrypt data in transit.

☒ Use Only for Privileged (Elevated Roles)

Audit logs are reviewed monthly to ensure that only authorized individuals have access to the system.

☐ Other: Specify.
Describe the control and the reason to impose it.

6.3. Retention of Information

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

☒ Yes.
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.

☐ No.
Explain why there is no NARA Records Schedule.

☐ A records retention schedule is in development.
Describe any relevant details such as the anticipated completion date or whether the schedule has been submitted to NARA and is waiting on approval.

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.
Click or tap here to enter text.
☐ 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: DEEOIC will permanently maintain records until 20 years after the last claim is paid (and there is no current sunset on our program) and after that all records will be transferred to NARA.

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/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

7.2. This system:

☐ Does not require an additional SORN beyond those identified above.
☐ Does not require a SORN. Provide explanation.
☐ Requires a new or additional SORN.
☒ Requires a modification to the following SORN(s):
DOL/OWCP-11, Office of Workers' Compensation Programs, Energy Employees Occupational Illness Compensation Program Act File

Reason for Modifying SORN(s):

☐ A significant increase in the number, type, or category of individuals about whom records are maintained.
Provide explanation.
☒ A change that expands the types or categories of information maintained.

New demographic information from the Voluntary Demographic form may be maintained in the systems covered by DOL/OWCP-11, Office of Workers' Compensation Programs, Energy Employees Occupational Illness Compensation Program Act File .

☐ A change that modifies the scope of the system.
For instance, the component agency decides to integrate information in one system that did not need a SORN with a system that does need a SORN.

☐ 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.
Identify the exemption here. Exemptions generally relate to when information is not required to be disclosed to an individual in connection with a Privacy Act request for their records. One of the most common exemptions relates to records collected and maintained in connection with law enforcement purposes. The three permissible exemptions are specifically identified in DOL's Privacy Act Regulations at 29 CFR 71.50, 71.51, and 71.52 and should be included in the applicable SORN(s).

☒ 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.

Demographic information from the Voluntary Demographic information form will result in new routine uses because the information is new to the systems.

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. A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number.

☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The types of harm that could be caused by a breach involving PII at the moderate impact level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail.

☐ **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. Any system that contains full SSNs must be listed as a "High" system due to the potential impact to the individual as a result of identity theft/fraud.

8.2. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

The Annual Cybersecurity and Privacy Awareness Training is mandatory for all federal employees and DOL contractors. It covers the basics of cybersecurity and privacy requirements within DOL and is considered adequate for the purposes of protection of PII within this system.

How Information is Acquired, Stored, and Shared

Acquisition: The Energy Program acquires new information via electronic and paper-based forms.

Storage: All OWCS components are hosted on the DOL GSS AWS Cloud, which has encryption of data-at-rest implemented. Access to the application is only provided on a need-to-know basis.

Shared: Energy Program data is only shared in accordance with the SORNs and per section 4.1 of this document.

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

The Energy Program allows limited access via the on-line web portal (ECOMP) to claimants to allow them to review their own information. User authentication is required to connect to ECOMP and users are limited to those records that pertain to their own claim(s). There is also an IVR system that is available to claimants to assist them with their claims and to determine claim status. The IVR system also requires authentication of callers before any information of a sensitive (PII) nature is discussed.

The systems only provide access to information on a need-to-know basis to ensure that users are given access only to the information that they are required to have access to for performance of their jobs. Logging of transactions and access is also done, and those logs are periodically reviewed to determine if attempts have been made to access data from either an outside source or an unauthorized user.

Protection against PII Breaches

Unauthorized Data Access:

The Energy Program allows limited access via the on-line web portal (ECOMP) to claimants to allow them to review their own information. User authentication is required to connect to ECOMP and users are limited to those records that pertain to their own claim(s). There is also an IVR system that is available to claimants to assist them with their claims and to determine claim status. The IVR system also requires authentication of callers before any information of a sensitive (PII) nature is discussed.

The systems only provide access to information on a need-to-know basis to ensure that users are given access only to the information that they are required to have access to for performance of their jobs. Logging of transactions and access is also done, and those logs are periodically reviewed to determine if attempts have been made to access data from either an outside source or an unauthorized user.

Potential Misuse of Data:

The Energy Program allows limited access via its on-line web portal ECOMP to claimants to allow them to review their own information. User authentication is required to connect to both ECOMP and users are limited to those records that pertain to their own claim(s). There is also an IVR system that is available to claimants to assist them with their claims and to determine claim status. The IVR system also requires authentication of callers before any information of a sensitive (PII) nature is discussed. The systems only provide access to information on a need-to-know basis to ensure that users are given access only to the information that they are required to have access to for performance of their jobs. Logging of transactions and access is also done, and those logs are periodically reviewed to determine if attempts have been made to access data from either an outside source or an unauthorized user.

Protecting Against Insider Threats:

The Energy Program provides access to its systems on a need-to-know basis. 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 Energy Program the ability to be more effective in preventing security vulnerabilities. Federal employees and contractors are required to do the Cybersecurity and Privacy Awareness Training and read the Rules of Behavior (ROB). Contractors are also required to sign a Non-Disclosure Agreement (NDA) before accessing the system. Also, at a minimum, a National Agency Check with Inquiries (NACI) is performed on all federal employees and contractors as part of the Personal Identity Verification (PIV) process.

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

The Energy Program uses the concept of least privilege as described above. This is implemented using various roles that have access only to the information that is required to perform a particular task. 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 Energy Program the ability to be more effective in preventing security vulnerabilities. DOL also implemented several IT controls (such as SSO, MFA, firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), encryption of data-at-rest (DAR), encryption of data-in-

transit, etc.) to prohibit unauthorized access from external parties. OWCP only collects the minimum information required to process claims.

Other: Identify any unique or heightened privacy risks associated with this system.

N/A

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

N/A

SIGNATURE PAGE

Reviewed by: **Click or tap here to enter text, *Insert Component Agency Acronym*** Representative

RACHEL POND Digitally signed by RACHEL POND
Date: 2024.10.09 15:31:13 -04'00'

Signature

Reviewed by: **Click or tap here to enter text**, DOL Privacy Program Representative

MARA BLUMENTHAL Digitally signed by MARA BLUMENTHAL
Date: 2024.10.09 16:08:08 -04'00'

Signature