OWCP Ombuds Office System

PRIVACY IMPACT ASSESSMENT

May 2024

■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: 2024.06.20 16:31:55 -04'00'

Carolyn Angus-Hornbuckle, Senior Agency Official for Privacy
Assistance Secretary for Administration and Management

Table of Contents

PRIVACY IMPACT ASSESSMENT

In accordance with Department of Labor (DOL) guidelines and the E-Government Act of 2002 (as amended), the Office of Workers' Compensation Programs (OWCP) and the Office of the Chief Information Officer (OCIO) conducted a Privacy Impact Assessment (PIA) on the OWCP Ombuds Office System because the system collects Personally Identifiable Information (PII).

1. OVERVIEW

- **The system name and the name of the DOL component(s) which own(s) the system.**

  Office of Workers' Compensation Program (OWCP) Ombuds Office System is considered a sub-component of the OWCP Workers' Compensation System (OWCS).

- **The purpose/function of the program, system, or technology and how it relates to the component's and DOL mission.**

  As a result of input received in town halls and focus groups OWCP has established an Ombuds Office to serve claimants and external interested parties who seek assistance with inquiries, individual concerns and achieving resolution to complaints related to the Division of Federal Employees', Longshore and Harbor Workers' Compensation (DFELHWC), and the Division of Coal Mine Workers' Compensation (DCMWC) programs. The Ombuds Office System will provide a mechanism for interested parties to submit inquiries and concerns. The system will also provide a method for the OWCP Ombuds Office to track inquiries and identify systemic issues impacting the customer experience.

- **A general description of the information in the system.**

  This system will contain the information gathered from the Ombuds Inquiry Form as submitted by claimants, their authorized representatives, or other members of the general public. This includes information about the specific issue or inquiry the person is requesting the Ombuds Office to research and may include some limited PII depending the nature of the inquiry.

- **A description of a typical transaction conducted on the system.**

  Users will fill out an online Inquiry Form, which is saved to a dedicated SharePoint repository where information is analyzed by the OWCP Ombuds Office staff. It is a one-way transaction and after submitting the form, the submitter no longer has access to the information in the form that was submitted. After submission, only notes about the status of the inquiry will be added to the SharePoint repository by designated Ombuds Office staff.

- **Any information sharing conducted by the program or system.**

  Information is strictly confidential and is only available to staff within the OWCP Ombuds Office on a need-to-know basis. In addition to DOL's Universal Routine Uses prescribed in the SORN, the Ombuds Office may disclose relevant and necessary information for purpose of resolving an inquiry or concern, if consent is given by the claimant or authorized representative to share. The Universal Routine Uses generally relate to matters where disclosure is needed in connection with legal proceedings or there is a compelling public interest for disclosure. Whenever possible, identifying information will be masked to preserve privacy when being shared.

- **A general description of the modules and subsystems, where relevant, and their functions.**

  This system consists of an online form on the front-end with a dedicated SharePoint repository as the back end to store the data from the form and allow the Ombuds Office staff to access the inquiry form information.

- **Please provide the legal authority to operate the program or system and collect PII.**

  30 U.S.C. 901 et seq., 20 CFR 725.1 et seq.
  33 U.S.C. 901 et seq. (20 CFR parts 701 et seq.); 36 DC Code 501 et seq.; 42 U.S.C. 1651 et seq.; 43 U.S.C. 1331 et seq.; 5 U.S.C. 8171 et seq.
  5 U.S.C. 8101 et seq., 20 CFR 1.1 et seq.

2. CHARACTERIZATION OF THE INFORMATION

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

- **From whom is information to be collected?**

  Individuals or their survivors who are seeking benefits from the OWCP's DFELHWC and DCMWC programs as well as the authorized representatives of those individuals. These consist of current federal employees, past federal employees, and members of the public.

- **Why is the PII being collected?**

  The system will provide a mechanism for the OWCP Ombuds Office to confidentially document and independently carry out the fulfillment of its duties in providing a service for claimants and external interested parties who seek assistance with inquiries and achieving resolution to individual concerns related to the DFELHWC and DCWMC

programs. The PII is being collected to verify identity and ensure the Ombuds Office has all the information needed to appropriately identify a claim file. The Ombuds Office is quasi-independent from other parts of OWCP, so the Ombuds Office is collecting this PII as its own source of information to be able to locate the appropriate claim file held by other parts of OWCP. The OWCP Ombuds Office is requesting a variety of different types of information to facilitate the identification of a particular claim in case the individual submitting the information does not have one or more pieces of information available that can assist in identifying a claim. The system will also provide a mechanism for the OWCP Ombuds Office to track and identify systemic issues impacting the customer experience.

- **What is the PII being collected, used, processed, stored, maintained, disseminated, or disposed of?**

  This system may collect and use the following information gathered from the Ombuds Inquiry Form:

  - Claimant First and Last Name
  - Claimant Date of Birth
  - OWCP Program
  - Claim Number/Case I.D./OWCP Number
  - Claimant Phone Number
  - Claimant Email Address
  - Claimant Home Address (street, city, state, zip code)
  - Authorized Representative First and Last Name (if applicable)
  - Authorized Representative Email Address (if applicable)
  - Inquiry/Concern Narrative

- **How is the PII collected?**

  Via online form, telephone, email.

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

  Forms are reviewed and checked for accuracy by the Ombuds Office staff and some of the information is cross-checked with information within one or more of OWCP's claims processing systems. System edit checks help to ensure the accuracy of the data on the forms.

- **Privacy Impact Analysis**

  There are many potential risks when PII is recorded about an individual, such as identity theft. The risk of PII being disclosed inadvertently 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. Additionally, this PIA will be reviewed periodically to continually monitor whether all the categories of information collected on the form continue to be necessary.

3. USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

- **Describe all the uses of the PII**

  The information is being collected on a form to file an inquiry, concern or complaint for action by the Ombuds Office. The information is being tracked to allow for noting follow-up actions and status of the inquiry. The data will also be analyzed to look for trends that can be used by OWCP to improve customer service.

- **What types of tools are used to analyze data and what type of data may be produced?**

  The data from the forms is manually analyzed by members of the OWCP Ombuds Office to look for trends that can allow for OWCP to improve the customer experience. OWCP may use spreadsheets and/or databases to assist in analysis, but at this time no automated tools are in use.

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

  No.

- **If the system uses commercial or publicly available data, please explain why and how it is used.**

  The system does not use commercial or publicly available data.

- **Will the use of PII create or modify a "system of records notification" under the Privacy Act?**

  Yes, the new SORN for this system is currently under development and has not yet been submitted to the Federal Register.

- **Privacy Impact Analysis**

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

Only Ombuds Office staff have access to the system. The system will use least privilege principles to ensure that only those who need access to the data to fulfill the mission are given access. All system users are required to read and sign the GSS Rules of Behavior before being granted access to the system and review these annually.

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?**

  Destroy when 5 years old or when no longer needed for reference.

- **Is a retention period established to minimize privacy risk?**

  Yes. NARA approved Record Control Schedules DAA-0271-2017-0002-0002

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

  Yes. NARA approved Record Control Schedules DAA-0271-2017-0002-0002

- **Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored, or maintained by the system if it is no longer required?**

  The Sharepoint repository will only contain the information collected on the Ombuds form, which is limited in scope. There is also no link between the Ombuds Office System and the claims systems in use for DFELHWC and DCMWC.

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

  Records will be destroyed after five years or whenever it is no longer needed to reference whichever is greater. A record would only be needed for reference past five years if it involved litigation that required the record to be maintained.

- **If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify, or anonymize PII.**

  While data is sitting at rest in the system, no efforts are being made to mask, de-identify, or anonymize PII. However, in disclosing or sharing information, whenever possible, identifying information will be masked to preserve privacy.

- **Privacy Impact Analysis**

  The information contained in the system is limited and access is also strictly controlled with only those with an absolute need to know having access to the information. Data will be deleted after 5 years unless it is required to be maintained for litigation purposes.

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?**

  Information is strictly confidential and is only available to staff within the OWCP Ombuds Office on a need-to-know basis. In addition to DOL's Universal Routine Uses prescribed in the SORN, the Ombuds Office may disclose relevant and necessary information for purpose of resolving an inquiry or concern, if consent is given by the claimant or authorized representative to facilitate a resolution to issues that claimants, their authorized representative, or other interest parties may have experienced in their claims process. The Universal Routine Uses generally relate to matters where disclosure is needed in connection with legal proceedings or there is a compelling public interest for disclosure. Whenever possible, identifying information will be masked to preserve privacy when being shared.

- **How is the PII transmitted or disclosed?**

  PII data will be disclosed only on a need-to-know basis dependent upon individual circumstances, if consent is given by the claimant or authorized representative. PII data that is disclosed will be transmitted electronically only to individuals authorized by the Ombuds Office to assist with resolution. There is no connection between the Ombuds Office System and the claims systems in use for DFELHWC and DCMWC.

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

  Data will be deleted after 5 years unless it is required to be maintained for litigation purposes.

- **Privacy Impact Analysis**

  Information is strictly confidential and is only shared with staff within the OWCP Ombuds Office on a need-to-know basis. In addition to the Universal Routine Uses prescribed in the SORN, the Ombuds Office may disclose relevant and necessary information for purpose of resolving an inquiry or concern about an OWCP claim, if consent is given by the claimant or authorized representative to share. Whenever possible, identifying information will be masked to preserve privacy when being shared.

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?**

  PII collected by the Ombuds Office will not be shared external to DOL, except where disclosure is required by law or court order as part of litigation.

- **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.**

  This is a new collection. PII collected by the Ombuds Office will not be shared external to DOL, except where disclosure is required by law or court order as part of litigation.

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

  In the event OWCP is compelled to share information externally due to litigation, transmission would be via encrypted email such as Kiteworks or via a secure transmission vehicle that meets all federal standards, such as the federal Advanced Encryption Standard (AES-128).

- **Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.**

  Not applicable.

- **How is the shared information secured by the recipient?**

  Any information shared would be as part of litigation and would be controlled by the court of jurisdiction.

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

  Not applicable. Direct access to the data is limited to only internal OWCP Ombuds staff.

- **Privacy Impact Analysis**

  The data is stored on secure servers within the DOL firewall and the servers and software where the data is stored are only accessible by internal DOL staff. Access to the data is limited to the OWCP Ombuds office reducing the risk of PII breach. Transmission would be limited to litigation actions which would normally be only a few records rather than the entire data set, further limiting exposure.

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? A notice may include a posted privacy policy, a Privacy Act Statement or notice on forms, or a system of records notice published in the Federal Register. If notice was not provided, please explain.**

  A Privacy Act Statement will be included on the online form. Individuals will be instructed to review the entire online form before submitting the form. The Privacy Act Statement will include a statement indicating that providing some or all of the information is voluntary and subject to the specific authorization to share information described below.

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

  Yes, we have the following statement included on the Ombuds Inquiry Form

  Do you give consent to OWCP Ombuds Office to share your identity, inquiry, concern with OWCP program staff and staff from other federal agencies for purpose of assisting with resolution? *Please note that inability to share this information may result in delay or inability to reach resolution to your concern.

  - ***Yes – unconditional*** *- you can share my identity and concern*
  - ***Yes – conditional*** *– you can share my concern but you may not share my identity*
  - ***No*** *– I do not wish to have my identity nor my concern shared*

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

  Yes. Individuals are asked to complete response on the Ombuds Inquiry form as to whether they give consent for their identity, inquiry, and concern to be shared.

- **Privacy Impact Analysis**

  A specific question requesting consent to share privacy data in order to help resolve inquiries and concerns is included on the Inquiry Form itself to ensure that all claimants have the right to consent or to decline consenting to their information being shared. In addition, a System of Records Notice (SORN) for this system will be published in the Federal Register. The Ombuds Form will also include a Privacy Act Statement to properly notify individuals of the privacy impact of providing information that will be collected in this system.

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?**

  Users will fill out an online Inquiry Form, which is saved to a dedicated SharePoint repository where information is analyzed by the OWCP Ombuds Office staff. It is a one-way transaction and after submitting the form, the submitter no longer has access to the information in the form that was submitted. Inquirers will receive correspondence from the Ombuds Office to discuss their inquiries, but that is outside this system.

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

  In addition to the rights as outlined in the Privacy Act, individuals can contact the OWCP Ombuds Office and provide amended information to the Inquiry Form they submitted at any time but will not have direct access to the original form.

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

  Claimants and their authorized representatives are provided their rights under the Privacy Act on the claim form that is filed. In addition, at the time they submit the Inquiry Form to the Ombuds Office, filers are informed that they should contact the OWCP Ombuds Office should there be any changes in the information provided on the Inquiry Form. OWCP Ombuds Office is also in regular communication with form submitters providing the opportunity for correction of information submitted on the Inquiry Form throughout the life of the inquiry or concern, until resolution is reached.

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

  Redress provided through the amendment process described above.

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.)**

  As an independent office within OWCP, the Ombuds Office maintains a database and records system that will not be disclosed to anyone besides applicable staff of the OWCP Ombuds Office on a need-to-know basis.

- **Will contractors to DOL have access to the system?**

  No. Only staff of the Ombuds Office will have access to the system.

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

  SharePoint has regular users and administrators. Administrators grant privileges to the regular users and are not users of the system themselves. Regular users are granted read and write access to allow for them to review the forms and add notes about the progress of their inquiry.

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

  OWCP and OCIO have put in place access control measures that include documented user access authorizations, encryption, and least privilege. Users request access through the DOL Service Now system where tickets are assigned to those with administrator access to the Share Point repository. Detailed access control, as well as other security control information is recorded in ServiceNow.

- **How are the actual assignments of roles and Rules of Behavior verified according to established security and auditing procedures? How often training is provided?**

  All DOL users are required to take the annual Cybersecurity and Privacy Awareness Training, which has a privacy module or component to it. OWCP has Rules of Behavior outlined for its major applications in addition to the GSS Rules of Behavior that apply to all uses of the DOL network.

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

  All DOL personnel are required to take the annual Cybersecurity 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?**

  All OWCP operations are required to have security audits and assessments conducted of their operations on an annual basis. All DOL 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 in February 2024. An ASA is performed every year on all systems.

- **Privacy Impact Analysis**

  The system resides on a secure server with assigned NIST 800-53 Rev. 5 security controls that will be inherited from OWCS, a parent system. The SharePoint repository has limited access to only Ombuds Office staff. Only the data received on the inquiry form and some notes on status are maintained in the data repository which also limits the potential exposure of PII.

10. TECHNOLOGY

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

- **Was the system built from the ground up or purchased and installed?**

  The system was purchased and installed. It consists only of Commercial Off The Shelf (COTS) products. MS Forms is being used to collect the information online and SharePoint is being used as the data repository.

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

  Considerations regarding data integrity, privacy, and security were analyzed and included in all decisions regarding the system. The use of secure servers, limiting communication to one-way from the inquirer to OWCP, and limitations on the amount of data collected were all considerations to improve security and privacy.

- **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 restricted access to the file storage location. OCIO also implemented several IT controls (such as a firewall, IDS, IPS, etc.) to prohibit unauthorized access from external parties.

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

  The system is made up of COTS products. No development is needed.

- **For systems in development, does the project employ technology which may raise privacy concerns? If so please discuss their implementation?**

  Yes. Rights to the data are granted only to Ombuds Office staff based on their duties. OWCP employs a checklist to ensure that when an individual either leaves their employment with OWCP or changes to a new position, their rights to systems are revoked.

11. PIA SIGNATURE PAGE

SHALONDA CAWTHON

Digitally signed by SHALONDA CAWTHON
Date: 2024.06.20 15:02:42 -04'00'

Reviewed by: Shalonda Cawthon, Component Agency Representative

MARA BLUMENTHAL

Digitally signed by MARA BLUMENTHAL
Date: 2024.06.20 15:27:30 -04'00'

Reviewed by: Mara Blumenthal, Privacy Program Representative