U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

PRIVACY IMPACT ASSESSMENT
eFILE/eSERVE

VERSION 1.8

8/5/2021

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/19/08	Privacy Impact Assessment Template 1.5	Adrienne Ramirez	Annual Update
05/01/10	Privacy Impact Assessment	Adrienne Ramirez, Michael O'Rourke	Annual Update
01/07/11	Privacy Impact Assessment	Adrienne Ramirez	Appendix A
3/12/12	Privacy Impact Assessment	Adrienne Ramirez	To include 3rd Party Website Updates
2/25/13	Privacy Impact Assessment	Adrienne Ramirez	Annual Review
12/16/15	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/16/16	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/18/17	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/17/18	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Update
11/27/20	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Updates

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
11/19/08	Privacy Impact Assessment Template 1.5	Tonya Manning
06/10/10	Privacy Impact Assessment Template 1.6	Tonya Manning
01/07/11	Privacy Impact Assessment Template 1.6	Tonya Manning
03/12/12	Privacy Impact Assessment Template 1.7	Tonya Manning
03/01/13	Privacy Impact Assessment Template 1.7	Tonya Manning
12/16/15	Privacy Impact Assessment Template 1.8	Miranda Key

12/16/16	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/20/17	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/18/18	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
11/27/20	**Privacy Impact Assessment 1.8**	**Adrienne Ramirez**

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

(To be completed for information systems containing PII)

1.1 OVERVIEW

The eFile/eServe system will enable public and Department of Labor users to electronically share, via filing and serving, case related information. The eFile/eServe system will modernize the legacy system through the replacement and/or elimination of current paper based case filing and serving systems. eFile/eServe will reside on a combination of the DOL Content Management Capability (DOL CMC), a DOL Platform as a Service (PaaS) and the DOL Case Management Platform (DOL CMP), an Appian Platform as a Service (PaaS) platform, which enables the DOL Office of Administrative Law Judges, Boards, and Solicitors office to achieve the following goals:

Implement an enterprise-level eFile/eServe solution:

- eFiling by providing case participants (Parties) and DOL stakeholders agencies (e.g. OALJ, the Boards, EBSA, ETA, OSHA, OLMS, WHD, and SOL) the ability to electronically file their case documents (e.g. appeal, exhibits, and correspondence, etc.) to the OALJ and the Boards (ARB, BRB, and ECAB); and
- eServing by providing administrative law judges and legal staff the ability to electronically serve judge-signed documents in a case.
- Public Portal for Registered Parties - Allow case representatives (Parties) to register and file their case documents (e.g., appeal, exhibits, and correspondence, etc.).
- Private Portal - Allow staff and contractors the ability to (1) approve case registrants and case filings, and serve judge-signed documents to a case to the Public Registered Parties Portal.

The eFile/eServe system will electronically integrate with the Office of Administrative Law Judges (OALJs) Case Tracking System (CTS), the boards' DOL Appeals system, and the OWCP Imaging System (OIS), which is the business process and tracking of the adjudication of cases.

1.2 CHARACTERIZATION OF THE INFORMATION

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

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

1. eFile/eServe collects non-sensitive PII on members of the public.

- From whom is information to be collected?

1. Members of the public

- Why is the Information being collected?

1. The information is being collected to allow case representatives (Parties) to register and file their case documents (e.g., appeal, exhibits, and correspondence, etc.).

- What is the PII being collected, used, disseminated, or maintained?
  1. PII data collected includes the users full name, title, organization/company, business address, business phone number, business e-mail address, and, if an attorney, they can provide the following optional information (bar number, certificate of understanding, and additional documents as they deem necessary).

- How is the PII collected?
  1. It is collected during the user registration process when the user initially registers into the system.

- How will the information collected from individuals or derived from the system be checked for accuracy?
  1. It is the user's responsibility to provide the correct information. When determining a case participant's rationale for accessing the system, the Department of Labor will review the user's information and confirm/deny that the information matches the information on record.

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?
  1. Privacy Act of 1974

- Privacy Impact Analysis
  1. A PIA is conducted because the system processes and stores non-sensitive PII of public users. OCIO will utilize various security controls such as SSL/TLS (encrypted data in transit), encrypted data-at-rest, and other controls to mitigate the risk of a data breach.

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
  1. The information is used to determine the eligibility of a case participant to electronically send and/or receive documents related to a specific case.

- What types of tools are used to analyze data and what type of data may be produced?
  1. Not applicable. Tools are not used to analyze the data.

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?
  1. eFile/eServe does not derive new data through aggregation of collected information.

- If the system uses commercial or publicly available data, please explain why and how it is used.
  1. The information collected is from the user during the registration process.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?
  1. Not applicable

- Privacy Impact Analysis
  1. OCIO has implemented various security controls to protect the data to include:
     a. Enabling SSL/TLS on websites for collection of data;
     b. Encrypting data at rest;
     c. Conducting Application vulnerability scans and remediating findings; and
     d. Conducting Security Impact Assessments prior to deploying code to Production

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?
  1. At this time of this publication, case related information is retained indefinitely. Cases can last years and the closed cases are used for documentation of the case and kept in case of an appeal.

- Is a retention period established to minimize privacy risk?
  Date (MM/DD/YYYY)
  1. No – the cases/documents could be reused even after the case is closed.

  Has the retention schedule been approved National Archives and Records Administration (NARA)? Provide the retention schedule number for the schedule utilized?
  1. Yes – eFile/eServe retention policy is based on the respective DOL systems for OALJ, the Boards, etc.

- 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?
  1. The cases/documents could be reused even after the case is closed so the PII is kept in the system.

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?
  1. No

- How is it determined that PII is no longer required?
  1. Not Applicable as the PII is retained for all cases/documents as it may be reused even after the case is closed.

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.
  1. eFile/eServe encrypts all data while in-transit and at-rest.

- Privacy Impact Analysis
  1. eFile/eServe encrypts all data while in-transit and at-rest. eFile/eServe also maintains an audit trail of data access and updates. Cases can be reused even after being closed so all PII is kept.

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?
  1. PII is not shared with internal organizations.

- How is the PII transmitted or disclosed?
  1. Not Applicable

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?
  {Include answer here}
  1. Not Applicable

- Privacy Impact Analysis
  1. Not Applicable

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?
  1. Not applicable. There is no external sharing of PII data.

- 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, provide the SORN ID in use for this system. . If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.
  1. Not applicable. There is no external sharing of PII data.

- How is the information shared outside the Department and what security measures safeguard its transmission?
  1. Not applicable. There is no external sharing of PII data.

- How is the information transmitted or disclosed?
  1. Not applicable. There is no external sharing of PII data.

- 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.
  1. Not applicable. There is no external sharing of PII data.

- How is the shared information secured by the recipient?
  1. Not applicable. There is no external sharing of PII data.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?
  1. Not applicable. There is no external sharing of PII data.

- Privacy Impact Analysis
  1. Not applicable. There is no external sharing of PII data.

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 or be prepared to provide a copy of the notice during an audit request. 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.
  1. The System of Records Notice (SORN) for each agencies applications have been published and are available for review.

- Do individuals have the opportunity and/or right to decline to provide information?
  1. Individuals can elect not to file and/or receive electronic case related information.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
  1. No

- Privacy Impact Analysis
  1. Individuals voluntarily provide their information as part of sending and/or receiving case related information.

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?
  1. Users input their information when registering in the eFile/eServe system. Users can update their personal information at any time in the application.

- What are the procedures for correcting inaccurate or erroneous information?
  1. Only the users can update their own information.

- How are individuals notified of the procedures for correcting their own information?
  1. Through website training.

- If no formal redress is provided, what alternatives are available to the individual?
  1. Not Applicable; There is a training provided to show the procedures of correcting their information.

- Privacy Impact Analysis
  1. A users personal information is inputted and managed only by that user. Training is provided for them to update their information.

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.)
  1. The OALJ internal employees and IT support.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA or be prepared to provide copies during an audit request
  1. Yes, for operations management purposes.

- Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.
  1. There are two roles assigned in the system listed below:
     a. System admin (IT support)
     b. Internal general users

- What procedures are in place to determine which users may access the system and are they documented?
  1. Public users are required to create accounts in the eFile/eServe system and will select a role, i.e. attorney, individual, attorney staff. Once registered, the user will then request access to a case of which they have interest. The appropriate Office of Administrative Judges (OALJ) or Boards users will then review the request and either approve or reject the request. If the request is approved, the user will then be able to submit and/or receive (be served) electronic files for the cases of which they are approved. If the request is rejected, the user will not be able to view and/or access any case related information. DOL users will be provided access based on completion of an account request via the DOL CMP Sharepoint account request process.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided. Provide date of last training.
  1. Once an accounts created, the user reviews and signs the rules of behavior. No system specific training is required to operate the system.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?
  1. DOL provides its users, federal and contractor, with Security Awareness training, at least annually, via LearningLink. eFile/eServe public users are provided with a link on the home page to the DOL Privacy and Security Statement web page (https://www.dol.gov/general/privacynotice)

- What auditing measures and technical safeguards are in place to prevent misuse of data?
  1. All user transactions, including access, will be captured in system audit logs.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?
  1. Yes, the ATO was completed on 8/10/2020.

- Privacy Impact Analysis
  1. The privacy risks for the eFile/eServe identified include inadvertent disclosure and misuse of confidential information. This risk is mitigated by the implementation, monitoring, and management of adequate access controls, end-to-end encryption, and assigning users with least privileges.

1.10 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?
  1. This system was purchased and installed

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.
  1. A risk assessment was conducted.

- What design choices were made to enhance privacy?
  1. No

- For systems in development, what stage of development is the system in, and what project development life cycle was used?
  1. The eFile/eServe system is operational

- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?
  1. Not Applicable

1.11 DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

OASAM has completed the PIA for eFile/eServe which is currently in operation. OASAM has determined that the safeguards and controls for this moderate system adequately protect the information.

OASAM 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

Chi Nguyen
System Owner

CHI NGUYEN Digitally signed by CHI NGUYEN Date: 2021.08.06 12:24:51 -04'00'

_____ _____

Signature of System Owner *Date*

Adrienne Ramirez
Privacy Officer, PO

ADRIENNE RAMIREZ Digitally signed by ADRIENNE RAMIREZ Date: 2021.08.17 08:31:59 -04'00'

_____ _____

Signature of Privacy Officer *Date*

Akosua Frimpong-Arhin
Information Security Officer, (ISO)

AKOSUA FRIMPONG-ARHIN Digitally signed by AKOSUA FRIMPONG-ARHIN Date: 2021.08.06 13:01:58 -04'00'

_____ _____

Signature of ISO *Date*

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for ☐ Federal employees, ☐ Contractor staff, ☐ Members of the Public {Check all that apply}

- ☐ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☐ First name ☐ Middle initial and/or ☐ Last name
- ☐ Name suffix such as Jr. Sr., etc.
- ☐ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☐ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☐ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ☐ Residential address
- ☐ Personal phone numbers (e.g., phone, fax, cell)

- ☐ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address
- ☐ Business address
- ☐ Business phone number (e.g., phone, fax, cell)
- ☐ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☐ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☐ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☐ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?
  {Please explain here}

- Is any part of this PII collection voluntary?
  {Please explain here}

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