U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

OCIO Electronic Records Management System (ERMS)

PRIVACY IMPACT ASSESSMENT

VERSION 1.8

DOCUMENT CHANGE HISTORY

Date	File name / 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
10/18/22	Privacy Impact Assessment	DISPP	Removal of PII Data Extract Guide question

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
3/12/12	Privacy Impact Assessment Template 1.7	Tonya Manning
3/1/13	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

12/18/2018	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
09/20/2023	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

1.1 OVERVIEW

Provide a thorough and clear overview, giving the reader the appropriate context in which to understand the responses in the PIA. The overview should contain the following elements for all systems that collect Personally Identifiable Information (PII) including third party websites and applications.

- **The system name and the name of the DOL component(s) which own(s) the system.**
  - The Department of Labor (DOL) Electronic Records Management System (ERMS) is owned by the Office of the Chief Information Officer (OCIO).
- **The purpose/function of the program, system, or technology and how it relates to the component's and DOL mission**
  - The ERMS facilitates the systematic management of DOL's temporary and permanent electronic records throughout their lifecycles. It brings DOL into compliance with OMB/NARA Memorandums M-19-21 and M-23-07 by providing the necessary infrastructure to support DOL's successful transition to fully electronic recordkeeping. As a records management modernization tool, the ERMS furthers OCIO's aim to provide information technology solutions and leadership that advance DOL's mission.
- **A general description of the information in the system**
  - The ERMS contains copies of federal records belonging to every DOL sub-agency except the Office of the Inspector General (OIG) and the Bureau of Labor Statistics (BLS). Copies of permanent and temporary records originating in agency SharePoint and OneDrive sites are stored in the ERMS. Copies of permanent records that are stored in other, more structured DOL information systems may also be ingested into the ERMS, although this is less likely if the originating system already has a mechanism for exporting record packages for transmittal to the National Archives and Records Administration (NARA). For temporary records stored in more structured DOL information systems, only metadata entries are ingested into the ERMS. The Department of Labor's records schedules (https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-labor) and the government-wide General Records Schedule (https://www.archives.gov/records-mgmt/grs) provide an overview of the possible informational content of records stored in the ERMS.
- **A description of a typical transaction conducted on the system.**
  Typical transactions in the ERMS occur in four stages:
  1. Categorization: Free-text disposition instructions from NARA-approved records schedule items are converted into programmatic rules by creating disposition categories in the Records Schedule module. Categories are not created every time a document enters the ERMS, but upon the approval or amendment of a new NARA-approved records schedule.
  2. Ingestion: Records and/or their associated metadata are ingested into the ERMS from agency information systems via RESTful API.
  3. Management: Agency Records Officers (AROs) apply disposition categories to their sub-agency's ingested records using location-driven categorization, manual categorization, or autocategorization. Records on legal hold are assigned to designated collections which prevent their deletion. The Departmental Records Officer may also use the Auditor iQ module to view activity reports from within the ERMS for the purposes of auditing, analysis, and other management actions.
  4. Disposition: AROs approve or defer record deletion and/or transfer to NARA. They package groups of records for transmission to NARA and download these packages as ZIP files.

- **Any information sharing conducted by the program or system.**
    - Routine internal information sharing occurs between DOL agencies and OCIO for the purposes of system maintenance and departmental records management. The system's architecture and user roles are configured so that agencies only have access to their own records. Routine external information sharing occurs with NARA for the purpose of permanent records transmittal. Information may also be shared externally with NARA or GAO for the purpose of records management inspections.

- **A general description of the modules and subsystems, where relevant, and their functions.**
    - FAST File Cabinets: Search and categorize files and metadata.
    - FeithDrive: Manage files ingested using FeithSync.
    - FeithSync: Ingest files from SharePoint and OneDrive via RESTful API.
    - Auditor iQ: Get real-time and historic activity reports from within the ERMS.
    - Auto Categorizer: Record categorization based on tailored SQL queries.
    - Records Schedules: Allows users to create and manage records disposition categories.
- **Where appropriate, a citation to the legal authority to operate the program or system.**
    - 36 CFR 1224: Records Disposition Programs (https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1224.)

- **A description of why the PIA is being conducted.**
    - No new information is collected by the ERMS. It stores copies of federal records and/or their metadata ingested from all DOL agencies except for OIG and BLS. A Privacy Impact Assessment (PIA) is being conducted because some of these records and metadata contain information collected by DOL sub-agencies which may include PII on Federal Employees, DOL Contractors, and members of the public.

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.**
    - The ERMS does not collect new PII. However, the copies of federal records and/or their metadata that the ERMS ingests for records management purposes may contain PII collected by DOL sub-agencies on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children. Temporary records existing on information systems other than SharePoint and OneDrive will not be copied over entirely into the ERMS, but rather managed via ingested metadata alone in order to limit PII in the ERMS. Temporary records existing on agency SharePoints and OneDrives will be fully ingested into the ERMS, but are less likely to contain PII than records in other, more structured information systems.
- **From whom is information to be collected?**
    - Information is collected from DOL sub-agency SharePoints, OneDrives, and other information systems where federal records are created or stored. No new information is collected by the ERMS, and all interactions with individuals for the purposes of collecting PII are conducted by DOL sub-agencies outside of the ERMS.

- **Why is the Information being collected?**
    - The ERMS does not collect any new information. However, it stores federal records and/or their metadata which contain information that DOL sub-agencies collected to support their missions and routine business functions. Information is stored on the ERMS in order to comply with OMB/NARA Memorandums M-19-21 and M-23-07. The ERMS makes it possible to accurately and efficiently manage temporary and permanent electronic records through the records lifecycle in a centralized manner.

- **What is the PII being collected, used, disseminated, or maintained?**
    - No PII will be collected, used, or disseminated by the ERMS. The ERMS maintains information collected by DOL sub-agencies in order to facilitate electronic records management to comply with OMB/NARA Memorandums M-19-21 and M-23-07. The ERMS may incidentally hold PII collected by DOL sub-agencies for business purposes. Any PII that may be in the ERMS is covered by separate SORNs and PIAs specific to the originating agency and system. Any PII that may be present in the system is maintained for an agency's business purposes but is managed according to disposition set by NARA-approved records schedules.
- **How is the PII collected?**
    - The ERMS does not collect PII, but it may incidentally ingest PII that is part of DOL federal records. Copies of records and/or their metadata are ingested into the ERMS by making calls to DOL information systems via RESTful API. All PII in the ERMS is collected by DOL sub-agencies in ways already outlined in existing SORNs and PIAs specific to the activity and sub-agency.
- **How will the information collected from individuals or derived from the system be checked for accuracy?**
    - It is the responsibility of DOL sub-agencies to check the accuracy of information they collect from individuals; their procedures for doing so are outlined in DOL's SORNs and PIAs. The ERMS simply aims to ingest accurate copies of DOL sub-agency record materials. Information is not changed from within the ERMS. However, the ERMS may update to reflect changes made to active records in their originating systems.

- **What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?**
    - No PII is collected by the ERMS. The collection of all PII that is stored within the ERMS is covered by legal authorities, arrangements, and/or agreements specified in published DOL SORNs and PIAs.

- **Privacy Impact Analysis**
    - The ERMS maintains record copies and/or metadata for DOL sub-agencies in order to create a more secure electronic records management environment at DOL. It is difficult to estimate the amount and type of PII that will be maintained within the system, as this will vary according to the business needs of DOL sub-agencies over time. However, the potential maintenance of PII by the ERMS does create the risk of unauthorized access and disclosure. This is mitigated by configuring and assigning user roles which limit user capabilities and information access according to their sub-agency affiliation and responsibilities. The ERMS also has highly configurable audit capabilities which allow the Departmental Records Officer (DRO) to monitor activity within the system as necessary to safeguard PII. Particularly in the case of records which originate in SharePoint or OneDrive, the ERMS provides greater access restriction and auditing capabilities than the originating system. By providing Agency Records Officers with the ability to simultaneously delete records from the ERMS and the originating system when their NARA-approved retention period has been met, the ERMS also helps mitigate the risk unauthorized access and disclosure across DOL systems by ensuring that information is not maintained for longer than necessary. Finally, by limiting the ingest of full record copies of the temporary records stored in information systems other than SharePoint and OneDrive, which are most likely to contain PII, the ERMS minimizes the scope and sensitivity of the PII it may store.

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**
    - The ERMS does not use PII, but merely stores records that may contain PII for DOL sub-agency recordkeeping purposes. PII that is collected by specific sub-agencies is used by those sub-agencies for mission-related activities and is covered under separate PIAs and SORNs.

- **What types of tools are used to analyze data and what type of data may be produced?**
    - The ERMS does not analyze data and does not produce new data.

- **Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?**
    - The system will not derive new data or create previously unavailable data about individuals through aggregation of collected information.

- **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?**
    - The potential storing of PII will not create or modify a system of records notification (SORN) under the Privacy Act. This is because the ERMS is not creating, collecting, using, disseminating, or aggregating new data or PII; it merely provides a centralized records management location for agencies to manage the proper disposition of their records according to DOL records schedules or the General Records Schedule. No information in the ERMS is retrieved by a personal identifier.

- **Privacy Impact Analysis**
  PII is handled according to agency business purposes and needs within its originating system; only authorized persons have access to records management copies in the ERMS. Those authorized are staff with records management responsibilities at the Departmental and sub-agency levels, and their access is limited to the information and capabilities that they need to perform their duties. Employees from one DOL sub-agency cannot view another sub-agency's records and vice versa. These controls ensure that any PII that may exist within the ERMS is handled solely to provide electronic management functionality to agencies.

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?**
  - Data in the ERMS is retained for the period specified by the applicable NARA-approved records schedule, links to which are provided below. Any data in the ERMS associated with records that have been placed under legal hold is retained for the hold's duration regardless of whether its retention period has expired. For DOL's records schedules see: https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-labor. For the most recent version of the General Records Schedule see: https://www.archives.gov/records-mgmt/grs.
- **Is a retention period established to minimize privacy risk?**
  - Yes, the retention period is established to minimize privacy risk.
- **Has the retention schedule been approved by the National Archives and Records Administration (NARA)?**
  - Yes. All data in the ERMS is covered by retention schedules approved by the National Archives and Records Administration.
- **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?**
  - When records in the ERMS reach their mandated deletion or accession date, they are automatically placed in an approval queue. Agency Records Officers (AROs) may then manually confirm that all requirements have been met for records to move into the next stage of disposition. This is typically deletion for temporary records and accession to NARA for permanent records (which entails a combined transfer and deletion action). When records are deleted from the ERMS, they may be simultaneously deleted from any originating systems linked to the ERMS. By providing the means to ensure that records are deleted across DOL systems when their retention periods end, the ERMS limits the amount of unnecessary PII that DOL maintains.
- **How is it determined that PII is no longer required?**
  - It is determined that a record containing PII is no longer required when the conditions outlined in the applicable NARA-approved records schedule for its deletion and/or accession to NARA have been met.
- **If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.**
  - The responsibility for masking, de-identifying, or anonymizing PII rests with the DOL sub-agencies who store their federal records in the ERMS. In order to maintain the integrity of federal records for recordkeeping purposes, the ERMS does not mask, de-identify, or anonymize PII. However, access to PII in the ERMS will be limited by a user's assigned role. In cases where agencies have taken measures to mask, de-identify or anonymize PII in the records' originating systems, record and/or metadata copies in the ERMS would reflect this intervention.

- **Privacy Impact Analysis**
  - The DOL records that pose the greatest privacy risk because of the PII they contain are generally temporary records stored in systems other than SharePoint and OneDrive. The privacy risk to the ERMS is greatly mitigated by only managing these temporary records within the system via their ingested metadata. When the ERMS does store PII it does so

with the aim of ensuring that the records in question are securely maintained for the duration of their legally mandated retention periods. Ultimately, the centralized deletion capabilities of the ERMS help mitigate the risks associated with keeping PII in information systems where deletion and/or transfer may not be easy to track and execute.

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?**
    - Routine information sharing occurs between DOL sub-agencies and OCIO for the purposes of ERMS maintenance and departmental records management. The ERMS's architecture and user roles are configured so that sub-agencies only have access to their own records. Information may additionally be shared with the DOL OIG for auditing purposes.
- **How is the PII transmitted or disclosed?**
    - PII is transmitted or disclosed through queries and screen displays within the ERMS.
- **Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?**
    - DOL sub-agencies in which records originate are responsible for reviewing the sharing of personal information and halting the transfer of sensitive information according to their business needs.
- **Privacy Impact Analysis**
    - There is no major privacy risk associated with the internal sharing and disclosure of PII through the ERMS. Potential risks have been mitigated by assigning users defined roles that limit their access to parts of the system relevant to their agency and responsibilities. Any internal information sharing that occurs between DOL agencies and OCIO is necessary to provide system maintenance and department-wide records management in order to comply with legally mandated electronic records disposition requirements.

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?**
  - PII associated with permanent records in the ERMS will be shared with NARA for the purpose of permanent record accession.
- **Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.**
  - Yes, the sharing of information outside the Department is compatible with the original collection. Sharing permanent records (including any PII they might contain) with NARA is legally mandated by 36 CFR 1224.10 (a) (https://www.ecfr.gov/current/title-36/chapter-XII/subchapter-B/part-1224). The process of sharing record material with NARA or GAO for the purposes of records management inspections is covered by section 5 of the Universal Routine Uses of Records within the General Provisions Applicable to All DOL Privacy Act Systems.
- **How is the information shared outside the Department and what security measures safeguard its transmission?**
  - Permanent records that may contain PII are shared with NARA through their Electronic Records Archives (ERA) Ingest Server or via portable media. Only Agency Records Officers have the user role permissions to download packaged records as ZIP files for the purposes of transmission to NARA.
- **How is the information transmitted or disclosed?**
  - Permanent records are transmitted in one of two ways. The ERMS packages the records for transfer in the form of a ZIP file. Agency records officers then download this ZIP file and either upload it to NARA's Electronic Records Archives (ERA) Ingest Server or transmit the file to NARA via portable media (hard drive, thumb drive, CD, or DVD).
- **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.**
  - No MOU, contract, or agreement that governs the sharing of PII in the ERMS is in place with any external organizations with whom information is shared.
- **How is the shared information secured by the recipient?**
  - When DOL accessions its permanent records (including those which may contain PII) to NARA, legal custody is also transferred. From this point forward, it is NARA's responsibility to maintain them in secure archival storage systems.
- **What type of training is required for users from agencies outside DOL prior to receiving access to the information?**
  - Not applicable. NARA staff who receive access to PII in permanent records accessioned from DOL do not interact with the ERMS.

- **Privacy Impact Analysis**
  - There are no new or major privacy risks identified in the external transmission or disclosure of PII from the ERMS. The transmission to NARA of permanent records containing PII is a legally mandated part of the records life cycle and would have happened even if the record

in question were never ingested into the ERMS. The privacy risk associated with transferring PII to NARA is mitigated by ERMS user role permissions that limit who can package and download ZIP files containing copies of records. The individuals with these permissions are trained Agency Records Officers. The ERMS's login requirements (identities are confirmed with users' PIV cards and users must be on DOL's internet network) additionally ensure that all ZIP file downloads and uploads to NARA's ERA Ingest Server take place in a secure environment.

1.7 NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

- **Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.**
    - Not applicable. The ERMS does not collect PII directly from individuals. The responsibility for providing notice to individuals prior to the collection of any PII that may be stored in the ERMS rests with the DOL sub-agencies who own the records' originating systems. For an overview of the notice that these originating systems provide to individuals, see the Department of Labor's Privacy Impact Assessments (https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy) and System of Records Notices (https://www.dol.gov/agencies/sol/privacy).

- **Do individuals have the opportunity and/or right to decline to provide information?**
    - Not applicable. Individuals do not provide information directly to the ERMS. Any opportunity individuals may have to decline to provide information occurs during the initial creation or submission of information at the DOL sub-agency level. It is the sub-agency's responsibility to provide this opportunity prior to their collection of any information that may become part of a federal record. For an overview of the opportunities that these originating systems give individuals to decline to provide information, see the Department of Labor's Privacy Impact Assessments (https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy) and System of Records Notices (https://www.dol.gov/agencies/sol/privacy).

- **Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?**
    - Not applicable. Individuals do not provide information directly to the ERMS. If they have the right to consent to particular uses of the information, these are determined at the sub-agency level and are specified in the relevant DOL PIA or SORN. The ERMS only uses the information it ingests for the purpose of federal records management compliance. All federal records in the ERMS are retained and disposed of according to publicly available, NARA-approved records schedules.

- **Privacy Impact Analysis**
    - No information is collected from individuals expressly for this system; all interactions with individuals take place at the sub-agency level. There is minimal risk associated with individuals being unaware of the placement of their information in the ERMS, because it executes records management disposition requirements that already applied to the submitted information in its originating system.

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?**
  - Not applicable. Procedures that allow individuals to gain access to their own information are managed directly through DOL sub-agencies rather than through the ERMS. The ERMS is not available to the public, and only those in DOL with the authorization outlined in Section 1.9 of this PIA have access to the system.
- **What are the procedures for correcting inaccurate or erroneous information?**
  - Not applicable. Procedures for correcting inaccurate or erroneous information occurs with the originating DOL sub-agency and originating system. Correction does not directly occur within the ERMS; if an active record copied into the ERMS is corrected or updated, its ERMS copy will update to reflect that correction.
- **How are individuals notified of the procedures for correcting their own information?**
  - Not applicable. Individuals are notified of the procedures for correcting their own information by the DOL sub-agency responsible for the originating system that collects and holds the individual's information.
- **If no formal redress is provided, what alternatives are available to the individual?**
  - Not applicable. Any alternatives to formal redress that may be available to the individual depend upon the DOL sub-agency and system that the records originate from, and are outlined in the system's applicable SORNs and/or PIAs. The ERMS does not provide either formal redress or alternatives, as it is a records management system and does not directly collect any information from individuals.
- **Privacy Impact Analysis**
  - There are no major privacy risks associated with individual access, redress, or correction. It is the responsibility of the DOL sub-agency that collected a piece of PII to provide the individual it pertains to with opportunities for access, correction, or redress. The ERMS does not have this authority, as it holds copies of records and/or their metadata on the behalf of sub-agencies for records management purposes.

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.)**
    - Records management staff at the departmental and sub-agency levels will have access to the ERMS. However, each user's capabilities and resource access within the system is tailored to match their records management responsibilities. For instance, the Departmental Records Officer (DRO) has complete administrative access to the ERMS. Meanwhile, Agency Records Officers (AROs) have full access to the records ingested from their sub-agency.
- **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.**
    - No, access to the information in the ERMS is limited to DOL records management staff.
- **Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.**
    - Yes, the ERMS assigns users a combination of "roles" and "groups" which respectively determine their capabilities and resource access within the system. Roles are separated into "Administrator," "Auditor," "FeithDrive" (which grants users permissions within the FeithDrive module), and "Records Manager." Groups provide user access to specific sets of records (for instance, all the ingested records for a single sub-agency). Each ERMS user is assigned a combination of roles and groups that corresponds to their records management responsibilities. For example, an ARO's account would be assigned the "Records Manager" role and the group for their sub-agency's records.
- **What procedures are in place to determine which users may access the system and are they documented?**
    - The DOL Records Management Office grants user access to the ERMS based on the verification of user records management responsibilities by sub-agency administrators.
- **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.**
    - User roles and groups are implemented by the Departmental Records Officer. Training is provided by the DOL Records Management Office on a rolling basis during implementation and when new users are authorized to access the ERMS. Auditing of these roles is accomplished by annual account revalidation training administered by the Departmental Records Management Office.
- **Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?**
    - Mandatory DOL Cybersecurity and Privacy Training is provided to all employees and contractors of DOL on an annual basis.
- **What auditing measures and technical safeguards are in place to prevent misuse of data?**
    - Within the ERMS there are specific user roles defined which provide varying levels of access to data stored in the ERMS. Additionally, auditing functionality exists within the ERMS's Auditor iQ Module. This module will facilitate the creation of a configurable dashboard which authorized users can monitor for irregularities within the system, such as abnormal access requests.
- **Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?**
    - Yes. The Security Assessment and Authorization was completed on 09/27/2022.
- **Privacy Impact Analysis**
    - Potential privacy risks to PII in the ERMS are mitigated by role-based access controls

which ensure that user access to information corresponds to their records management responsibilities. Although role-based access cannot completely guarantee that misuse of the ERMS will not occur, conducting annual account revalidation training and maintaining audit logs to check for irregularities such as abnormal access requests mitigates this risk.

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?**
  - The system was purchased and installed.
- **Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.**
  - Data integrity, privacy and security were analyzed during the ERMS Authority to Operate (ATO) assessment process. FIPS 199 categorization identified the ERMS as MODERATE impact, meaning that "the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."[1] This identification determined which security controls were applicable to the ERMS.
- **What design choices were made to enhance privacy?**
  - Encryption technologies, role-based access control, and identity authentication were implemented in the ERMS to enhance privacy.
- **For systems in development, what stage of development is the system in, and what project development life cycle was used?**
  - Not applicable, as the ERMS is not in development.
- **For systems in development, does the project employ technology which may raise privacy concerns? If so, please discuss their implementation?**
  - No, the ERMS does not employ technology which may raise privacy concerns.

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

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 Electronic Records Management System (ERMS) 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

Steven Pierce
System Owner

Steven Pierce Digitally signed by Steven Pierce
Date: 2024.02.15 15:43:27 -05'00'

_____ _____

Signature of System Owner *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
- ☒ 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)

- [x] Mailing address (e.g., P.O. Box)
- [x] Personal e-mail address
- [x] Business address
- [x] Business phone number (e.g., phone, fax, cell)
- [x] Business e-mail address
- [ ] Medical information including physician's notes
- [ ] Medical record number
- [ ] Device identifiers (e.g., pacemaker, hearing aid)
- [x] 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? **N/A**
- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system? **N/A**

APPENDIX B: ERMS SYSTEM TRACKING TEMPLATE

Program/System:
List the name of the agency, program office, and name of the system within [insert Name of main System].

Purpose and Use:
Provide a general description of the program/system and its purpose, including how the purpose of the program/system relates to DOL's mission and how the system operates/business process.

Legal Authority:
What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

System Access:
Provide a general description of who has access to the system.

Individuals Impacted:
Provide a list of individuals (i.e., members of the public) whose information will be contained in the system.

Sources of Information:
Provide the sources from which information maintained in the system is derived.

Data Elements:
*Provide a specific description of information that may be collected, maintained, and/or generated by the system. Highlight any collection and maintenance of PII and Sensitiv*e PII.

SORN Coverage:
List the SORN(s) under which this data collection and maintenance is covered.

Records Retention Period:
List the retention period(s) for records maintained in the system.