PRIVACY IMPACT ASSESSMENT

Effective Date: September 16, 2024

Employee Benefits Security Administration (EBSA)
Retirement Savings Lost and Found Database (RSLF)

☑ 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: 2024.09.19 11:18:13 -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, EBSA 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)

Name of System

Retirement Savings Lost and Found Database (RSLF)

Location of the System

RSLF is hosted on DOL's Drupal Web Content Management System (WCMS) which resides on OCIO's Amazon Web Service (AWS).

Brief Description of the System

Section 523 of the Employee Retirement Income Security Act (ERISA), as added by the SECURE 2.0 Act of 2022, requires the Department of Labor (DOL) to create an online searchable database called the "Retirement Savings Lost and Found" within two years of the enactment date. The system is designed to help individuals who may have lost track of a retirement plan to search for the contact information of the plan administrator in order to make a claim with the plan administrator for benefits owed to them.

The Retirement Savings Lost and Found Database (RSLF) is a secure online database that contains information about individuals who are, or were, participants in certain workplace-sponsored retirement plans. It has two portals: a public portal and an intake portal. The public portal allows individuals to search for information that enables them to locate the administrator of any plan with respect to which they are or were a participant. The intake portal allows plan administrators or authorized plan record keepers, to upload data into the database. In addition to data received directly from plan administrators, DOL will also receive benefit data on plan participants from the Social Security Administration (SSA). This data is submitted to SSA annually via the 8955-SSA Form and will be transferred to DOL through a separate secure file transfer process. The SSA data will be extracted by SSA

from its 8955-SSA database and securely delivered to EBSA as structured/tabular data in CSV file format.

Both portals use Login.gov to grant and manage user access. The public portal requires users to enter their Social Security number (SSN) as the search parameter. If positive results are found, the contact information of the plan administrator holding the benefits is displayed to authenticated users. No other information will be displayed, except as required by SSA. If no results are found, a negative results message is displayed.

Individuals will also be providing information to the DOL if they choose to opt-out of having their information available through the RSLF searchable public portal.

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: Specify

This System is operated by:

☒ Component agency: Employee Benefits Security Administration (EBSA)

☐ 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). The RSLF is expected to have two associated Information Collection Requests (ICRs). One is for the voluntary collection of information from plan administrators and for the "Opt-Out" collection from individuals.

☐ A change to the PII Confidentiality Impact Level (NIST SP 800-122) or System Security Categorization (NIST SP 800-60 and FIPS 199).

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

☒ General Public
☒ Contractors (Contractors will not be working with the data that comes from SSA).
☒ Government Employees
☒ Other: Plan administrators for retirement plans described in section 523 of ERISA.

1. INFORMATION IN THE SYSTEM

Employee Benefit Security Administration (EBSA) collects certain types of information from certain sources using the 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
☐ Date of Birth
☐ Place of Birth
☒ Email
☐ Citizenship
☒ Social Security number (Full)
☒ Social Security number (Truncated form for Opt-out)
☒ Financial Information (i.e., defined benefit plan - periodic payment, defined
☐ Driver's License
☐ Financial Account
☒ Taxpayer ID (EIN)
☐ Passport Number
☐ Gender
☒ Telephone Number (opt-out only)
☐ Criminal Record
☐ Education
☐ Age
☐ Financial Transaction
☐ Employer ID
☐ Alien Registration Number
☐ Vehicle Identifier
☐ Employee ID
☐ Credit Card
☐ Medical Record
☐ File/Case ID
contribution plan- total value of account
☐ 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
☐ Plan administrator and Plan Sponsor Telephone Number
☐ Proprietary or Business Information
☐ Employment Performance Ratings
☒ Plan Administrator and Plan Sponsor Address
☐ Work History
☐ Procurement or contracting records
☐ Other Performance Information
☐ Fingerprints
☐ Scars, Marks, Tattoos
☒ Signatures of Plan Sponsor/Administrator
☐ 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: Form 8955-SSA data - participants who separated with a deferred vested benefit; name/EIN and Plan Number of previous plan administrator or plan sponsor; SSA-specified codes (i.e., A, B, C, D) for types of benefits owed or dispersed benefits.

1.2. The information is collected using the following methods:

☒ Website-based forms
☐ Paper forms
☒ Electronic forms
☒ Verbal collection (only in connection with EBSA Benefit Advisors providing individual assistance in response to inquiries related to RSLF)
☐ 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 for individual Opt-Outs)
☒ Telephone (assistance provided to individuals by EBSA Benefit Advisors)
☐ Email
☐ Legal or other representative: Specify.
☐ Other: Specify.

Government Sources:

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

Non-government Sources:

☐ Public Organizations
☒ Private Sector (Plan administrators and plan sponsors through the DOL Intake Portal as well as via the Login.gov authentication process)
☐ Commercial Data Brokers
☐ Third Party Website or Application
☐ Other: Specify.

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?

Section 303 of the SECURE 2.0 Act of 2022, which was enacted on December 29, 2022 (SECURE 2.0) amended ERISA to add Section 523. Paragraph (e) section 523 of ERISA specifically authorizes the collection of SSNs by its reference to "taxpayer identifying number" which generally refers to an SSN for U.S. citizens or those of lawful alien status. This provision is also memorialized in the United States Code at 29 U.S.C. 1153(e).

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

DOL will collect SSNs from the Social Security Administration and plan administrators to create the statutorily required searchable database that links particular individuals to a particular plan administrator who may have information for the individual to locate unclaimed retirement assets.

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

The collection of SSNs is required by section 523 of ERISA, so no alternatives were considered.

1.4.4. The alternatives were not selected because:

The collection of SSNs is required by section 523 of ERISA.

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. There is not yet an OMB control for the ICR associated with the voluntary collection of information from plan administrators.

☒ The information collected is part of an existing collection and the OMB control number for the collection is: The information collection for the Opt-Out will be covered in an update to OMB Control Number 1210-0146.

☐ 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 Department is collecting information to establish the RSLF as required in section 523 of ERISA to allow an individual to search for information that enables the individual to locate the administrator of any plan described in Section 523 with respect to which the individual is or was a participant or beneficiary and provide contact information for the administrator of any such plan.

Data on unclaimed benefits will be coming from 2 different sources: (1) the Plan Administrator intake portal, and (2) Form 8955-SSA data being transferred to DOL by SSA. The Form 8955-SSA data is Federal Tax Information (FTI) subject to 26 U.S.C. 6103 disclosure restrictions. Processing and storage of these two datasets will be via separate databases.

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:

Section 303 of the SECURE 2.0 Act of 2022 (Consolidated Appropriations Act, 2023, Pub. L. 117-328, Division T, Title III – Simplification and Clarification of Retirement Plan Rules); 136 Stat. 4459; 29 U.S.C. 1153.

Agreements covering the information to be shared by SSA with DOL are in development and will be identified in this PIA after the agreements are finalized.

3. INTENDED USE OF THE INFORMATION

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

To allow an individual to search for information that enables the individual to locate the administrator of any plan with respect to which the individual is or was a participant or beneficiary to assist the individual in obtaining unclaimed retirement assets. Information will also be collected to track individual opt-out requests.

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

☒ Yes: Individuals who opt-out will have limited PII (First Name, Last Name, last four of Social Security number) included in an opt-out database which will be used to exclude data from the publicly

searchable RSLF. The opt-out database will work in tandem with the RSLF participant data to exclude results from public searchability.

☐ No

4. INFORMATION SHARING AND ACCESS

4.1. Will EBSA engage in sharing of data internally within DOL or externally?

☒ Yes, the PII in the system will be shared with or by EBSA.

☐ No, the PII in the system will not be shared with or by EBSA.

Internal Sharing

Component Agency	Information Shared	Purpose
Office of the Inspector General	All necessary information to support the mandated audit in section 523(g) of ERISA	Statutorily required audit.

External Sharing

Organization	Information Shared	Purpose	MOU or other Agreement
Individual public users	Plan administrator contact information	To assist the individual in locating unclaimed retirement assets.	Not applicable.
Social Security Administration	SSA will provide relevant information from the Form 8955-SSA to DOL.	To provide searchable data for the RSLF	Under development at SSA. No actual participant information will be received from SSA until an agreement is executed. Test data may be provided to coordinate data transfer processes in advance.

4.2. Does EBSA place a limitation on re-dissemination of PII shared with internal or external organizations?

Internal Sharing

☒ Yes, there are limitations placed on the re-dissemination of PII.

Personnel from DOL's OIG are expected to be provided data or granted limited-term access to data in the RSLF to support the audit required in section 523 of ERISA (annually for the first 5 years and then every 5 years thereafter). The corresponding report to Congress will not contain any PII. EBSA will not be sharing data with any other component agencies. However, system administrators within DOL's OCIO who provide ongoing operation and maintenance of the RSLF will have access to the data in the RSLF. No PII may be re-disseminated.

☐ 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, EBSA does not share PII with other DOL component agencies.

External Sharing by EBSA

☐ Yes, the external agency or entity is required to verify with the DOL component agency before re-dissemination of PII.
Explain here.

☒ No. External sharing with the individuals who are attempting to locate lost retirement assets is required by section 523 of ERISA. Although the information pertaining to a plan administrator that is provided to an individual after a positive match in RSLF may not be considered PII on its own, it is only provided after an element of sensitive PII (SSN) is input by the individual user. DOL does not place any limitations on how the identity-verified individual uses information obtained from a positive search result because that information is only pertaining to that individual. However, to protect RSLF from being used inappropriately or fraudulently to link specific individuals to the existence of unclaimed retirement assets, RSLF relies upon identity verification at the IAL2-level (the person requesting access must provide evidence that they are the owner of the identity they are claiming) before allowing an individual to search for benefits. An individual will only be able to see information that is matched to their verified SSN.

☐ 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.

This system will connect with Login.gov, which is operated by the General Services Administration. Information received from Login.gov to verify user credentials and verify identity will only be used for a limited period of time, tied to each log-in session.

☐ 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:

The Privacy Act Statement will be provided on the public and intake portals for RSLF. The Privacy Act Statement on the Ask EBSA online webform will be updated to account for the new SORN and Opt-out.

☐ 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.

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

☒ Other: Plan administrators are not required to provide PII directly to DOL as part of the voluntary collection. If a plan administrator chooses to provide information to the DOL about an individual, the individual will not have the opportunity to decline to have the information provided. Neither plan administrators nor individuals will be able to decline to have SSA provide their Form 8955-SSA data to DOL.

However, section 523 of ERISA requires DOL to allow any individual to contact the Secretary to opt out of inclusion in the RSLF. This will be done through the existing Ask EBSA online webform (OMB

Control Number: 1210-0146). In order to opt out, individuals will select a checkbox to opt-out from data being included in the RSLF and must provide their first and last name and the last 4 digits of their SSN. Although the opt-out is optional, the individual may not decline to provide the requested information that is needed to honor an opt-out request. Opt-out requests will go from the Ask EBSA webform to DOL OCIO staff directly so that it can be matched with any data in the RSLF and suppressed from showing in searches.

5.3. Do individuals have an opportunity to consent to particular uses of their PII?

☐ Yes.

☐ No.

☒ Other: An individual's consent is limited to the opt-out. Although their data will be suppressed from being publicly searchable, it will not be deleted from the RSLF. Individuals who do not opt-out will be subject to the uses described in Section 523 of ERISA, uses described in this PIA, and the routine uses described in the associated SORN for RSLF. Section 523 of ERISA indicates that DOL may use or disclose information collected for RSLF only to assist an individual in locating a plan administrator with respect to which the individual is or was a participant or beneficiary and may disclose such information only to such employees of DOL whose official duties relate to that purpose.

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 will

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

☒ Other: Individuals will be limited to: (1) opting out from data being included in the RSLF public search and (2) the rights provided under the Privacy Act of 1974, as detailed in the SORN for this system.

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 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 Office 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 public portal users and intake portal users are subject to the rules of behavior that appear on the respective portal before logging in, which includes the penalties for committing an offense identified in 18 U.S.C. section 1030. Plan administrator intake portal users are also provided notice regarding punishment for unlawful statements to an agency of the United States as indicated in 18 U.S.C. 1001(a) and 29 U.S.C. 666(g).

☒ All DOL users are subject to a Code of Conduct that includes the requirement to protect PII from disclosure to unauthorized persons or groups.

The Code of Conduct is provided in the *Department of Labor OCIO Managed IT Systems Rules of Behavior (ROB), Version 6*

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

DOL provides annual Cybersecurity and Privacy Awareness training to all personnel. Records are kept through DOL's LearningLink platform.

☐ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices.
Identify and describe the specific roles that receive role-based training, including how it is tracked and monitored.

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

DOL personnel with access to the database that contains the Federal Tax Information (FTI) received from the SSA will be required to take IRS Security Awareness training initially and annually. The training is offered and tracked through EBSA's Blackboard learning site with records of all EBSA training being maintained in the DOL Learning Link system.

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

As required by ERISA section 523, DOL may disclose SSA-provided information (Form 8955-SSA data is considered FTI) in RSLF only to such employees of the Department of Labor whose official duties relate to the purpose described in the law. Data received from plan administrators via the intake portal is limited to DOL employees and contractors whose official duties relate to the purpose described in the section 523 of ERISA.

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

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

A security assessment report was completed on July 31, 2024.

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

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

DOL entered into a contract with PTG-WebFirst, LLC for RSLF Portal Support Services. The contract includes provisions to deal with protection of PII, training, and PII Incident/Breach response. Contractors are strictly prohibited from having access to FTI per IRS/SSA requirements.

☐ Contracts with customers establish DOL ownership rights over data including PII.
Identify the contract(s) and describe the included provisions.

☐ Other: Specify.
Describe.

6.2. Technological controls for the system:

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

For security purposes and to be able to monitor improper use of the RSLF, external system access is tracked using system logs of the intake and public portals.

☒ User Log In Credentials

DOL system administrators: access to the RSLF requires DOL network login and an account to access the RSLF. DOL system administrators access the RSLF using government furnished computers which require a Personal Identity Verification card to login.

EBSA Benefit Advisors: will have access to RSLF data through searching on transaction number that public users will receive in (1) search of RSLF search (both successful and unsuccessful searches) and (2) opting-out from data being included in Lost & Found Search through the ask EBSA webform.

Intake Portal Users: access requires a Login.gov account (with associated multi-factor authentication) *and* an EFAST User ID.

Public portal users: access requires a Login.gov account that must meet IAL2 identity verification requirements with an associated multi-factor authentication of the account (AAL2).

☒ Zero Trust Access Framework

For DOL content editors, database administrators, and Drupal administrators, DOL uses the Zscaler Private Access (ZPA) service which provides zero trust capabilities to internally accessed applications and services.

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

☒ Encryption of Data at Rest

The RSLF uses the industry standard AES-256 encryption algorithm to encrypt data.

☐ Firewall
Click or tap here to enter explanation.

☒ Role-based Access Controls

A limited number of EBSA personnel have access to the Drupal webpage content to make any necessary updates to the public and intake portals. This user role does not have access to the underlying PII in the RSLF.

EBSA Benefit Advisors will have access to RSLF data through searching on a transaction number that public users will receive in (1) search of RSLF search (both successful and unsuccessful searches) and (2) opting-out from data being included in Lost & Found Search through the Ask EBSA webform.

A limited number of OCIO contractor system administrators (PTG-Webfirst and/or Microsystems Automation Group, MSAG) will have access to read-only database views and read/write access to the actual database tables. Contractor access will be limited to voluntary plan administrator-uploaded data through the intake portal. Per IRS restriction, contractors will not have access to the database containing FTI.

Only DOL employee system administrators will have read and/or write access to data obtained from SSA from Form 8955-SSA.

Intake portal users are only permitted to upload data. They are not able to access the data after it is uploaded.

Public portal users are limited to the single input of an SSN and the output of plan administrator contact information, which is only provided to identity verified individuals. No additional information from the RSLF is provided or accessible.

☒ Encryption of Data in Transit

Data passed from the intake portal or public portal users to the application is protected via HTTPS/SSL encryption and data from the database to the public portal user is protected by TLS encryption.

Form 8955-SSA data transmitted to DOL by SSA will be transferred via a DOL-approved Secure File Transfer tool, which will provide encryption in transit and at rest.

☒ Use Only for Privileged Users (Elevated Roles)

The RSLF also uses certain privileged user roles with additional security protections for database administrators, Drupal administrators, and system administrators.

☐ 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.
Identify the applicable NARA Records Schedule(s).
☐ No.
Explain why there is no NARA Records Schedule.
☒ A records retention schedule is in development.

Records will not be destroyed until a records retention schedule is developed. However all records retention activities will remain in compliance with the final Records Schedule.

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: DOL has no plans to dispose of data received in connection with the RSLF.

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 additional information.

7.1. This system is covered by one or more existing SORNs.

There is no existing SORN but one is under development. Upon finalization of the new SORN for this system, it will be identified in an update to this PIA.

7.2. This system:

☒ Does not require an additional SORN beyond those identified above.
☐ Does not require a SORN. Provide explanation.
☐ Requires an additional new SORN.
☐ Requires a modification to the following SORN(s):
Identify the SORNs here.

8. ANALYSIS OF PRIVACY RISK

8.1. PII Confidentiality Impact Level from NIST Special Publication 800-122

Indicate the potential impact 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.
☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐ **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.

8.2. FIPS 199 Security Categorization

Indicate the overall system security categorization from the FIPS 199 assessment.

☐ **Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

☐ **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.

8.3. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

Inadequate training related to systems that deal with PII has the potential to lead to a variety of privacy compliance failures, including PII breaches, discussed in more detail below.

DOL is minimizing the potential for privacy compliance failures related to DOL personnel and related privacy risks by ensuring that all DOL personnel who have access to this system receive system-specific training.

DOL employee system administrators will receive initial and annual IRS Security Awareness training (part of the IRS Safeguards program which applies to handling FTI) and DOL-specific PII Breach Response Training. DOL contractors who have access to data submitted through the intake portal (non-FTI) will receive PII Breach Response Training.

EBSA Benefit Advisors will receive IRS Security Awareness training (part of the IRS Safeguards program).

All DOL personnel, regardless of their role, receive annual DOL Cybersecurity and Privacy Awareness training.

How Information is Acquired, Stored, and Shared

Information that is not encrypted while in transit and at rest is at heightened risk of being usable by unauthorized system intrusions. Sharing information with unvalidated users and without monitoring system use increases the risk that information is being used/shared improperly.

Transport Layer Security (a cryptographic protocol) v1.2 or higher encryption is used on the public portal where individual users input their SSN to ensure data in transit is encrypted. The public portal masks an SSN as it is typed into the search field to avoid inadvertent disclosure.

Multi-factor authentication through Login.gov enables identification of the intake portal users from whom PII is collected and public portal users searching RSLF.

The AWS cloud service has built-in encryption of data at rest for all data in RSLF to reduce the likelihood that unauthorized system intrusions would lead to usable data that could be exposed to the public

domain. These protocols also apply to the opt-out table that houses the first name, last name, and last 4 digits of an individual's SSN.

Form 8955-SSA data transmitted to DOL by SSA will be transferred via a DOL-approved Secure File Transfer tool, which will provide encryption in transit and at rest. This data will be stored in a separate database from Plan Administrator-provided data sent via the Intake portal.

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

DOL uses a FEDRAMP-certified cloud service provider to ensure the proper encryption mechanisms are incorporated into RSLF. DOL chose to use data masking of SSNs as they are input into the search parameter of the public portal due to the heightened sensitivity of this PII data element.

Protection against PII Breaches

Unauthorized Data Access:

As with all systems that provide a publicly accessible portal, there is a risk of external attacks or attempts to access data using improper means. To protect against this risk, public portal users will not be allowed to run a search and/or receive search results unless they have their identity verified at an IAL2 level and linked with the SSN. The search results page was designed to display only the information to a public portal user needed to locate a plan administrator who was matched to the input SSN. This minimizes the potential for improper data access.

Intake portal users (i.e., plan administrators) will be required to have IAL1 level credentials and provide their EFAST2 User ID to verify their authorization and authenticity to upload plan participant data.

Uploaded data is encrypted both at rest and in transit to ensure the integrity of the information and prevent usable data from being extracted due to certain types of system breaches.

Potential Misuse of Data:

DOL users who have access to the database represent a possible privacy risk if they are not properly informed and trained on the requirements to only use information in the system as provided in law, policies, and related privacy-compliance documents. As identified above, DOL users are provided with general awareness and system-specific privacy training (based on their roles) to ensure they understand the importance of only using RSLF and the data to which they have access for authorized purposes.

Public portal users have limited access to the RSLF database to minimize the potential for misuse. Additionally, DOL utilizes data masking as individuals input an SSN and encryption of all data stored in the system. Any data that an individual obtains from RSLF (i.e., plan administrator contact information) is data pertaining to themselves (after identity verification) that is needed to properly locate unclaimed retirement funds.

The intake portal for plan administrators is designed only for uploading text files in CSV format. Plan administrators will not be able to access the file after it is uploaded to prevent improper data access/alterations. If a plan administrator realizes a mistake may have been made, they will be able to upload another file with the correct data and it will supersede (but not overwrite) the previous uploaded data.

Protecting Against Insider Threats:

If a DOL insider engages in unauthorized activity, system administrators can immediately discontinue access for the particular user. DOL reduces this risk by using access control Standard Operating Procedures that ensure only certain users are granted access upon approval and only to certain data in RSLF, based on the principle of least privilege. DOL monitors use through system logs which can help identify suspicious activity. Additionally, the system-specific training provided to RSLF DOL users with direct access to PII emphasizes the importance of reporting PII breaches (which includes unauthorized use of RSLF and/or the data within RSLF). All DOL users are informed of their obligation to report suspected or actual PII breaches immediately.

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

As DOL was developing the RSLF, a variety of choices were made to mitigate the possible privacy risks associated with PII Breaches. For instance, DOL originally considered using another system, EFAST2, as a portal to upload data. However, this would create additional privacy risks due to the interaction between two DOL systems. DOL decided to create an intake portal for plan administrators to directly upon data to RSLF.

DOL also explored the various options related to identity verification and multi-factor authentication in connection with the use of Login.gov. Due to the risk of fraudulent accounts being used with the public portal by relying only upon IAL1 identity verification (self-certification), DOL relies upon an IAL2-level of identity verification (which for RSLF requires documentation proving identity which is linked to a particular SSN) before a user can search the system. This is consistent with IRS requirements related to accessing FTI. Likewise, to avoid spoofed or fraudulent data being uploaded to RSLF through the intake portal, DOL requires the EFAST2 User ID to verify an individual acting on behalf of a plan administrator is authorized to submit data.

Opt-out support will also be provided to the public using the existing Ask EBSA webform (OMB Control Number: 1210-0146). Users will select a checkbox to opt-out from data being included in Lost & Found Search and enter their first name, last name, and last 4 digits of their SSN. The Opt-Out will be routed to DOL OCIO staff directly to suppress the data from showing in searches.

Other Risks: DOL will be collecting additional PII from individuals in support of the Opt-Out. Although this information will be stored in an additional table for the RSLF, DOL will be collecting the minimum information it believes will be necessary to properly locate records pertaining to the individual (First name, Last name, last 4 digits of SSN) in order to honor an Opt-Out request.

DOL does not plan to dispose of any information collected in connection with the RSLF.

SIGNATURE PAGE

Reviewed by: EBSA Representative

Leyla Mansur Digitally signed by Leyla Mansur
Date: 2024.09.18 10:43:15 -04'00'

Signature