entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Files are stored electronically. Users will fill out an online Inquiry Form, which is saved to a dedicated SharePoint repository where information is analyzed by the OWCP Ombuds Office staff. It is a one-way transaction and after submitting the form, the submitter no longer has access to the information in the form that was submitted. The SharePoint repository is stored on the DOL Azure Cloud with periodic backup of the data to protect against system failure or loss. Other than backups there are no copies of the data stored outside the DOL Azure Cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by claimant's name, claim number/ID number, program, and/or date of birth.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The system maintains only PII that is necessary and relevant to accomplish the purpose for which it is being collected. It will be destroyed when 5 years old or when no longer needed for reference based on NARA approved Record Control Schedules DAA–0271–2017–0002–0002.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DOL uses a role-based access for the system's SharePoint files where only those expressly granted access by the system administrator can see the folder where the information is stored. Users can be granted read only or read/write access and access will be granted only to authorized personnel from the Ombud's Office. DOL works with Microsoft to ensure the security of the cloud environment. Controls include but are not limited to, firewalls, least privilege, role-based access, and two factor authentication. DOL assigns NIST 800–53 control requirements to the system.

RECORD ACCESS PROCEDURES:

If an individual wishes to access their own records in the system, the individual should contact OWCP directly and follow the instructions for making a Privacy Act Request on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting records under the Privacy Act in regulations at 29 CFR 71.2. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

CONTESTING RECORD PROCEDURES:

If an individual wishes to request a correction or amendment of a record, the individual should direct their request to OWCP directly. The request must be in writing and must identify:

- The name of the individual making the request,
- The particular record in question,
- The correction or amendment sought,
- The justification for the change, and
- Any other pertinent information to help identify the file.

Additional information can be found on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting a correction or amendment at 29 CFR 71.9. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

NOTIFICATION PROCEDURES:

If an individual wishes to know if a system contains information about the individual, the individual should contact OWCP directly and follow the instructions for making a Privacy Act Request on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting records under the Privacy Act in regulations at 29 CFR 71.2. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None. This is a new System of Records.

Signed at Washington, DC.

Carolyn Angus-Hornbuckle,

Assistant Secretary for Administration and Management.

[FR Doc. 2024–25410 Filed 10–31–24; 8:45 am]

BILLING CODE 4510–CK–P

DEPARTMENT OF LABOR

Privacy Act of 1974; System of Records

AGENCY: Employee Benefit Security Administration (EBSA), Department of Labor.

ACTION: Notice of a new system of records.

SUMMARY: The Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A–108 requires that each agency publish notice of a new or modified system of records that it maintains. 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.'' This notice proposes a new system of records for the Retirement Savings Lost and Found that contains information about individuals who are or were participants in certain workplace-sponsored retirement plans. The system is designed to help individuals who may have lost track of their retirement plan search for the contact information of the appropriate plan administrator and make a claim for benefits owed to them.

DATES: Comments must be received no later than December 2, 2024. This new SORN is effective upon publication of this Notice. If no public comments are received, the routine uses will be effective beginning December 2, 2024. If the DOL receives public comments, the DOL will review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: We invite you to submit comments on this notice. You may submit comments by any of the following methods:

- *Email: ebsa.opr@dol.gov.*
- *Mail, hand delivery, or courier:* U.S. Department of Labor, Employee Benefits Security Administration, Office of Research and Analysis, Attention: PRA Officer, 200 Constitution Avenue NW, Room N–5718. In your comment, specify RSLF SORN.

FOR FURTHER INFORMATION CONTACT: To submit general questions about the system of records, contact Stephen Sklenar by email at *sklenar.stephen.m@dol.gov* or by phone at (202) 693–8500.

SUPPLEMENTARY INFORMATION: Section 523 of the Employee Retirement Income Security Act (ERISA), as added by the SECURE 2.0 Act of 2022,[1] requires the Department of Labor (DOL) to create an online searchable database called the ''Retirement Savings Lost and Found'' (RSLF). The RSLF is designed to help individuals who may have lost track of a retirement plan to search for the

[1] *See* Consolidated Appropriations Act, 2023, Public Law 117–328, division T, title III—Simplification and Clarification of Retirement Plan Rules, section 303; 136 Stat. 4459.

contact information of the plan administrator in order to make a claim with the plan administrator for benefits owed to them.

The 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. Plan administrators or authorized plan record keepers are not required to submit this information to DOL. Uploading any such data is strictly voluntary.

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 in plan administrator-provided data, the name and contact information of the plan administrator holding the benefits is displayed to authenticated users. No other information will be displayed. If no results are found, a negative results message is displayed.

In addition to data received directly from plan administrators, DOL will also receive benefit data on plan participants from the Social Security Administration (SSA) that is reported to SSA annually via the 8955–SSA Form. The SSA data will be extracted by SSA from its 8955–SSA database and securely delivered to EBSA as structured/tabular data in a common (*e.g.,* CSV) file format. If positive results are found in SSA-provided data, the name and contact information of the plan administrator holding the benefits and benefit information (*e.g.,* year reported, amount, type of annuity (if applicable), payment frequency, units/shares and account value(s)) is displayed to authenticated users. If no results are found, a negative results message is displayed.

Individuals will also be able to opt-out of having their data searchable. Limited information (*e.g.,* name, last 4 digits of SSN) used to match the opt-out request to any data in the RSLF, will be collected from individuals and stored in a separate opt-out table.

SYSTEM NAME AND NUMBER:

Retirement Savings Lost and Found, DOL/EBSA–16.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for the system of records is Employee Benefits Security Administration, 200 Constitution Ave. NW, Washington, DC. The system resides on DOL's secure cloud and data center computing infrastructure.

SYSTEM MANAGER(S):

Director, Office of Program Planning and Performance Evaluation (OPPEM), Employee Benefits Security Administration, 200 Constitution Ave. NW, Washington, DC, 20210.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 523 of ERISA (29 U.S.C. 1153).

PURPOSE(S) OF THE SYSTEM:

The RSLF is an online searchable database designed to help individuals who may have lost track of retirement plan assets to search for the contact information of the associated plan administrator and make a claim with the plan administrator for benefits owed to them.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are or were a participant or beneficiary who may have vested, unclaimed retirement benefits with a plan to which the vesting standards of section 203 of ERISA (29 U.S.C. 1053) apply.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information about individuals who have vested retirement benefits with a plan to which the vesting standards of section 203 of ERISA (29 U.S.C. 1053) apply. The records include the participant's first name, middle initial, last name, Social Security number, the name of the plan, plan number, plan sponsor name, plan sponsor Employer Identification Number (EIN), plan sponsor phone number, plan administrator name, plan administrator EIN, plan administrator phone number, plan administrator address, participant Social Security Number (SSN), and participant name. The records also include benefit data on plan participants from the Social Security Administration (SSA) that is reported to SSA annually via the 8955–SSA Form including: benefit information—*e.g.,* year reported, amount, type of annuity (if applicable), payment frequency, units/shares and account value(s).

Individual who opt-out of the RSLF will have their first name, last name, and last 4 digits of SSN stored by DOL in an opt-out table.

RECORD SOURCE CATEGORIES:

The Social Security Administration (SSA) will provide DOL with information from IRS Form 8955–SSA filings, which plans are required to file each year.

The administrator of a plan described in 29 U.S.C. 1053 may voluntarily provide information about individuals who are 65 or older directly to DOL through the intake portal.

Individuals will provide information to DOL if they elect to opt-out of the RSLF.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974 at 5 U.S.C. 552a(b) and the uses described in section 523 of ERISA (29 U.S.C. 1153), under which DOL may disclose information from this system of records without the consent of the individual.

1. To appropriate agencies, entities, and persons when (a) DOL suspects or has confirmed that there has been a breach of the system of records; (b) DOL has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOL (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOL's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

2. To another Federal agency or Federal entity, when DOL determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

3. To contractors and employees of contractors who have been engaged to assist the agency in the performance of or working on a contract or other activity or service for the RSLF. However, no disclosure of data provided to DOL by SSA (from IRS Form 8955–SSA filings) will be made to contractors or employees of contractors. Disclosure will be limited to plan administrator-provided data.

Note: Recipients will be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a; see also 5 U.S.C. 552a(m).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The records are stored within secure databases that reside within the U.S. Department of Labor's secure cloud and data center computing infrastructure.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Individuals searching for lost retirement benefits retrieve data from the system through the uses of a web-based search form which queries the databases, but must use Login.gov to obtain a credential that verifies that the individual is properly identity-proofed. 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. Members of the application support team will have the ability to retrieve information from the databases in order to perform data validation and integrity checks.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records received from SSA will be retained in accordance with statutory requirements and consistent with SSA's own records schedules associated with this data. These SSA retention policies include:

1. *Master Files of Social Security Number (SSN) Holders and SSN Applications, 60–0058* which classifies the records as ''TEMPORARY, [to] destroy 300 years after date of enumeration, or when no longer needed for Agency business, whichever is later.''

2. *Earnings Recording and Self-Employment Income System, 60–0059* which classifies the records as ''Temporary [to] delete/destroy the Earnings Recording and Self-Employment Income System record on an individual's SSN 300 years after the number holder's date of birth.''

If required, DOL will establish its own NARA Records Schedule apart from the above SSA schedules to remain consistent with their requirements. Plan administrator-provided data will adhere to the same retention timeframes.

All records will be disposed of in accordance with the DOL guidelines, NARA records retention schedule(s), and IRS Publication 1075, as applicable. For the 1075-covered data (*i.e.,* data received from SSA), DOL will dispose of data according to guidance in IRS Publication 1075.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOL systems security and privacy policies. All DOL users are subject to a Code of Conduct that includes the requirement for confidentiality. DOL Personnel (employees, contractors, interns, volunteers) receive annual training on privacy and confidentiality policies and practices. Access to the PII is restricted to authorized personnel only. Appropriate NIST security and privacy controls for protecting PII are imposed. DOL users access the portal using government furnished computers which require a Personal Identity Verification card to login. Public users (IAL2-level identity authenticated) and Plan Administrator users rely upon *Login.gov* credentials for access. All data is encrypted at rest and in transit.

RECORD ACCESS PROCEDURES:

If an individual wishes to access their own data in the system, the individual should contact EBSA directly and follow the instructions for making a Privacy Act Request on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting records under the Privacy Act in regulations at 29 CFR 71.2. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

CONTESTING RECORD PROCEDURES:

If an individual wishes to request a correction or amendment of a record, the individual should send their request to EBSA directly. The request must be in writing and must identify:

- The name of the individual making the request,
- The particular record in question,
- The correction or amendment sought,
- The justification for the change, and
- Any other pertinent information to help identify the file.

Additional information can be found on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting a correction or amendment at 29 CFR 71.9. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

NOTIFICATION PROCEDURES:

If an individual wishes to know if a system contains information about the individual, the individual should contact EBSA directly and follow the instructions for making a Privacy Act Request on the DOL's web page at: *https://www.dol.gov/general/privacy/instructions.* The DOL also describes its process for requesting records under the Privacy Act in regulations at 29 CFR 71.2. Individuals who need additional assistance may also reach out to the DOL's Privacy Office by email at *privacy@dol.gov.*

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Carolyn Angus-Hornbuckle,

Assistant Secretary for Administration and Management.

[FR Doc. 2024–25405 Filed 10–31–24; 8:45 am]

BILLING CODE 4510–29–P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[NASA Document No: NASA–24–076]

Astrophysics Advisory Committee; Correction

AGENCY: National Aeronautics and Space Administration.

ACTION: Notice of meeting, correction.

SUMMARY: NASA published a document in the **Federal Register** on October 29, 2024 concerning an Astrophysics Advisory Committee Meeting. The document needs to be updated to add language regarding the need to publish this notice less than 15 calendar days before meeting date.

FOR FURTHER INFORMATION CONTACT: Jamie Krauk, 202–358–5210.

SUPPLEMENTARY INFORMATION:

Correction

In the **Federal Register** of October 29, 2024, in FR Doc. 2024–25082, on page 85989, in the second column, add a final paragraph to the **SUPPLEMENTARY INFORMATION** section to read:

''Per § 102–3.150(b) of the FACA Final Rule, this notification is published with fewer than 15 calendar days notice as a result of exceptional circumstances that required substantive changes due to recent cybersecurity incidents.''

Emily Pellegrino,

Program Analyst, NASA Directives and Regulations.

[FR Doc. 2024–25459 Filed 10–31–24; 8:45 am]

BILLING CODE P