

12. To another Federal agency or Federal entity, when we determine 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.

13. To third parties when an individual involved with a request needs assistance to communicate because of a hearing impairment or a language barrier (e.g., to interpreters, telecommunications relay system operators).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

We will maintain records in this system in electronic and paper form.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

We retrieve records in this system by SSN, name of the requesting member of the public, or both SSN and name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

In accordance with NARA rules codified at 36 CFR 1225.16, we maintain records in accordance with agency-wide Legal Bucket, DAA-0047-2022-0003.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

We retain electronic and paper records containing personal identifiers in secure storage areas accessible only by our authorized individuals, including our employees and contractors, who have a need for the information when performing their official duties. Security measures include, but are not limited to, the use of codes and profiles, personal identification numbers and passwords, and personal identification verification cards. We restrict access to specific correspondence within the system based on assigned roles and authorized users. We use audit mechanisms to record sensitive transactions as an additional measure to protect information from unauthorized disclosure or modification.

We annually provide authorized individuals, including our employees and contractors, with appropriate security awareness training that includes reminders about the need to protect PII and the criminal penalties that apply to unauthorized access to, or

disclosure of, PII (5 U.S.C. 552a(i)(1)). Furthermore, authorized individuals with access to databases maintaining PII must annually sign a sanctions document that acknowledges their accountability for inappropriately accessing or disclosing such information.

RECORD ACCESS PROCEDURES:

Individuals may submit requests for information about whether this system contains a record about them by submitting a written request to the system manager at the above address, which includes their name, SSN, or other information that may be in this system of records that will identify them. Individuals requesting notification of, or access to, a record by mail must include: (1) a notarized statement to us to verify their identity; or (2) must certify in the request that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

Individuals requesting notification of, or access to, records in person must provide their name, SSN, or other information that may be in this system of records that will identify them, as well as provide an identity document, preferably with a photograph, such as a driver's license. Individuals lacking identification documents sufficient to establish their identity must certify in writing that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

CONTESTING RECORD PROCEDURES:

Same as record access procedures. Individuals should also reasonably identify the record, specify the information they are contesting, and state the corrective action sought and the reasons for the correction with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant. These procedures are in accordance with our regulations at 20 CFR 401.65(a).

NOTIFICATION PROCEDURES:

Same as records access procedures. These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

79 FR 34558 (June 17, 2014), RAMP.

83 FR 54969 (November 1, 2018), RAMP.

[FR Doc. 2026-00816 Filed 1-15-26; 8:45 am]

BILLING CODE 4191-02-P

SOCIAL SECURITY ADMINISTRATION

[Docket No. SSA-2024-0017]

Privacy Act of 1974; Matching Program; Correction

AGENCY: Social Security Administration (SSA).

ACTION: Notice of a new matching program; correction.

SUMMARY: We published a new matching program in the **Federal Register** on October 15, 2024 concerning a matching program with the States, including tribal agencies and United States territories. That document contained an incorrect date on which the matching program would be applicable. This notice corrects that error.

FOR FURTHER INFORMATION CONTACT:

Interested parties may submit general questions to Andrea Huseh, Division Director, Privacy and Disclosure Policy, Law and Policy, Social Security Administration, 6401 Security Boulevard, Baltimore, MD 21235-6401, at telephone: (410) 965-6868, or send an email to Andrea.Huseh@ssa.gov.

SUPPLEMENTARY INFORMATION: Correction.

On October 15, 2024, we published a new matching program in the **Federal Register** (89 FR 83071). The **DATES** section of the October 15, 2024 notice stated, "The matching program will be applicable on November 14, 2024, or once a minimum of 30 days after publication of this notice has elapsed, whichever is later." This notice corrects the **DATES** section to state, "The matching program will be applicable on January 1, 2025, or once a minimum of 30 days after publication of this notice has elapsed, whichever is later." This correction aligns the dates in the **Federal Register** with the correct dates specified in the signed agreements between SSA and the States.

Matthew Ramsey,

Head of Privacy and Disclosure Policy, Law and Policy.

[FR Doc. 2026-00814 Filed 1-15-26; 8:45 am]

BILLING CODE P