4191-02-P

SOCIAL SECURITY ADMINISTRATION

[Docket No. SSA-2022-0023]

Privacy Act of 1974; System of Records

AGENCY: Social Security Administration (SSA).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, we are issuing public notice of our intent to modify an existing system of records entitled, Repository of Electronic Authentication Data Master File (60-0373). This notice publishes details of the system as set forth below under the caption, SUPPLEMENTARY INFORMATION.

DATES: The system of records notice (SORN) is applicable upon its publication in today's *Federal Register*, with the exception of the new routine uses, which are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

We invite public comment on the routine uses or other aspects of this SORN. In accordance with the Privacy Act of 1974, we are providing the public a 30-day period in which to submit comments. Therefore, please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress may comment on this publication by writing to the Executive Director, Office of Privacy and Disclosure, Office of the General Counsel, SSA, Room G-401 West High Rise, 6401 Security Boulevard, Baltimore, Maryland 21235-6401, or through the Federal e-Rulemaking Portal at http://www.regulations.gov. Please reference docket number SSA-2022-0023. All comments we receive will be available for public inspection at the above address and we will post them to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Melissa Bellitto, Government Information Specialist, Privacy Implementation Division, Office of Privacy and Disclosure, Office of the General Counsel, SSA, Room G-401 West High Rise, 6401 Security Boulevard, Baltimore, Maryland 21235-6401, telephone: (410) 966-5855, email: Melissa.M.Bellitto@ssa.gov.

SUPPLEMENTARY INFORMATION: We are modifying this SORN to accurately reflect the information we collect and to further support advancing our objectives in continuing and expanding our digital identity processes. We are modifying the system of records name from "Repository of Electronic Authentication Data Master File" to "Digital Identity File Record System." We are adding two new routine uses 1) to permit disclosures to the Internal Revenue Service (IRS), for auditing purposes of the safeguard provisions of Internal Revenue Code (IRC) of 1986; and 2) to permit disclosures to IRS concerning the digital identity associated with electronic wage submissions processed by SSA under section 232 of the Social Security Act. We are revising routine use No. 3 to incorporate gender-inclusive language, in support of EO 13988, "Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation." Finally, we are clarifying the language in existing routine use No. 4 for easier reading.

In addition, this modification reflects enhancements to our digital identity processes that utilize single sign-on, account management, and second factor authentication information required by digital identity guidance and requirements from the National Institute of Standards and Technology (NIST), OMB, and the Presidential Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." These enhancements include the evolving use of third-party credential service providers to ensure secure access to our online services and enable us to move towards a shared federated identity management platform. To reflect these enhancements, we are modifying the category of records maintained in this system to

provide more clarity to the data we collect as we have updated and expanded our digital identity processes. We are also modifying the category of individuals and purpose of the system to more accurately cover the individuals and uses covered by this system.

Lastly, we are modifying the notice throughout to correct miscellaneous stylistic formatting and typographical errors of the previously published notice, and to ensure the language reads consistently across multiple systems. We are republishing the entire notice for ease of reference.

In accordance with 5 U.S.C. 552a(r), we provided a report to OMB and Congress on this modified system of records.

Matthew Ramsey,

Executive Director,
Office of Privacy and Disclosure,
Office of the General Counsel.

SYSTEM NAME AND NUMBER: Digital Identity File Record System, 60-0373

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION:

Social Security Administration

Office of Digital Transformation

Robert M. Ball Building

6401 Security Boulevard

Baltimore, MD 21235

SYSTEM MANAGER(S):

Social Security Administration

Chief Information Officer

Robert M. Ball Building

6401 Security Boulevard

Baltimore, MD 21235

(410) 966-5855

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Sections 205(a) and 702(a)(5) of the Social Security Act (Act), as amended, and the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283).

PURPOSE(S) OF THE SYSTEM: We will use the information in this system to assist with SSA's digital identity processes and for auditing purposes. Digital identity includes functions necessary to establish the identity of individuals or an individual interacting with us on behalf of another individual, agency, or entity who are seeking access to our digital programs, services, and applications through online, electronic, automated, and telephone services. Digital identity functions include identity proofing, credential issuance and revocation, authentication, identity federation, access controls, preference management, and credential management. When real-world identity is necessary for a

given digital service, SSA must be able to determine, with confidence, that individuals are who they claim to be through identity proofing.

We may use information in this system to assist SSA (or other Federal agencies when applicable) to prevent or stop suspected or confirmed fraud or inappropriate usage of SSA's online services. We may also use contact information (e.g., email addresses) from individuals who have gone through the digital identity process for program outreach (e.g., notification about our programs, online services, and SSA events) and other purposes related to our administration of the Social Security Act.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system maintains information from individuals who interact with our digital programs, services, and applications regardless of whether the individuals are interacting with us on their own behalf or are interacting with us on behalf of another individual, agency, or entity. This system covers anyone who we require to obtain a digital identity to conduct a transaction with us, including when we use a credential service provider (CSP), an identity provider (IdP), or other authorized third party to perform some or all credential management services (e.g., prove identity, manage authentication credentials, and authenticate users).

CATEGORIES OF RECORDS IN THE SYSTEM: We will maintain information needed for digital identity processes dependent on the digital program, service, or application, as well as maintain archived transaction and historical data. Examples of information that we maintain for digital identity include, but are not limited to, the following:

- Name (last, first, middle, and suffix);
- Date of birth;
- Place of birth;
- Banking information including financial account number and/or routing

number;

- Postal address(es);
- Address(es) from W-2 and Schedule-Self Employed (SE) forms;
- Phone number;
- Email address;
- Mother's surname at birth (sometimes referred to as mother's maiden name);
- Social Security number (SSN);
- Driver's license or state-issued identification number and issuing State or equivalent;
- Images of the identity evidence (e.g., driver's license);
- Employer name and Employer Identification Number (EIN) for business and government services;
- Blocked account status;
- Failed access data;
- Effective date of passwords; and
- Other data that allows us to evaluate the system's effectiveness.

We may maintain information that we or the authorized CSP, IdP, or third party collects to register, issue, and maintain the credential (e.g., to administer multi-factor authentication), including verified attributes the authorized CSP, IdP, or third party maintains or passes to us after a user successfully passes identity proofing, such as:

- Identity attributes such as name, full or partial SSN, and date of birth;
- Email address;
- User ID;
- Phone numbers (primary, alternate, mobile, home, work, and/or landline);

- Level of access;
- Transaction ID;
- Pass/fail indicator;
- Date/time of the transaction;
- Codes associated with the transaction;
- Level of confidence in the provided identity and attributes, including indicators of potential risk factors;
- Type of authenticators (e.g., password);
- Self-generated security questions and answers; and
- The identity of the organization and/or individual representative or employee performing the identity proofing.

Other program-specific attribute information that we, a CSP, an IdP, or other third party collects directly, or on behalf of us, may include:

- Citizenship;
- Accepted terms of service (Y/N);
- Employment information such as job title, job role, and organization;
- Business and affiliations;
- Address (e.g., postal address, home address, business address(es);
- Justification/nomination for access to our computers, networks, or systems;
- Supervisor/nominator's name, job title, organization, phone numbers, and email address;
- Verification of training requirements or other prerequisite requirements for access to our computers, networks, or systems; and
- Government-issued identity document type, number, and expiration date; and

- Authorization for access to information when necessary.

We also maintain records on access to our computers, networks, online programs, and applications, including:

- User ID and passwords;
- Registration numbers or IDs associated with our Information Technology (IT) resources;
- Date and time of access;
- Logs of activity interacting with our IT resources;
- Internet Protocol (IP) address of access;
- Web browser and device information collected from the device used to access IT services, including a device fingerprint;
- Logs of internet activity;
- Track opt-in and opt-out of electronic messaging selections;
- Records on the authentication of the access request, names, phone numbers of other contacts, and positions or business/organizational affiliations and titles of individuals who can verify that the individual seeking access has a need to access the system; and
- Other contact information provided to the agency or that is derived from other sources to facilitate authorized access to SSA IT resources.

RECORD SOURCE CATEGORIES: We obtain information in this system of records from individuals seeking access to a service provided by SSA that requires digital identity. We also obtain information from existing SSA systems of records, CSPs, IdPs, authorized third parties, Federal, State, or local agencies, and SSA contractors.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: We will disclose records pursuant to the following routine uses; however, we will not disclose any

information defined as "return or return information" under 26 U.S.C. 6103 of the IRC, unless authorized by statute, the Internal Revenue Service (IRS), or IRS regulations.

1. To the Office of the President, in response to an inquiry received from that office made on behalf of, and at the request of, the subject of record or a third party acting on the subject's behalf.
2. To a congressional office in response to an inquiry from that office made on behalf of, and at the request of, the subject of the record or a third party acting on the subject's behalf.
3. To the Department of Justice (DOJ), a court or other tribunal, or another party before such court or tribunal, when:
   (a) SSA, or any component thereof; or
   (b) any SSA employee in their official capacity; or
   (c) any SSA employee in their individual capacity where DOJ (or SSA where it is authorized to do so) has agreed to represent the employee; or
   (d) the United States or any agency thereof where we determine the litigation is likely to affect SSA or any of its components, SSA is a party to the litigation or has an interest in such litigation, and SSA determines that the use of such records by DOJ, a court or other tribunal, or another party before the tribunal is relevant and necessary to the litigation, provided, however, that in each case, we determine that such disclosure is compatible with the purpose for which the records were collected.
4. To contractors and other Federal agencies, as necessary, for assisting SSA in the efficient administration of its programs. We will disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist in accomplishing an agency function relating to this system of records.

5. To student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for SSA, as authorized by law, and they need access to personally identifiable information (PII) in our records in order to perform their assigned agency functions.
6. To the DOJ for investigating and prosecuting violations of the Social Security Act.
7. To the National Archives and Records Administration (NARA) under 44 U.SC. 2904 and 2906.
8. To appropriate agencies, entities, and persons when:
   (a) SSA suspects or has confirmed that there has been a breach of the system of records;
   (b) SSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, SSA (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 SSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
9. To another Federal agency or Federal entity, when SSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:
   (a) responding to 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.

10. To IRS, Department of the Treasury, for the purpose of auditing SSA's compliance with the safeguard provisions of the IRC of 1986, as amended.
11. To IRS, Department of the Treasury, digital identity information associated with electronic wage submissions processed by SSA under section 232 of the Social Security Act for the purpose of investigating fraud, abuse, or security risks in such wage submissions.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: We will maintain records in this system in electronic form.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: We will retrieve records in this system by the individual's name and associated identifying information, SSN, as well as internal transaction and credential identifiers (e.g., transaction identification for the internet benefit application, transaction identification for an electronic online Direct Deposit change, etc.).

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 approved NARA General Records Schedules (GRS) 3.2, item 031; GRS 5.2, item 020; and GRS 4.2, item 130.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: We retain electronic files containing personal identifiers in secure storage areas accessible only by our authorized employees 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 will use audit mechanisms to record sensitive transactions as an additional measure to protect information from unauthorized disclosure or modification.

We annually provide 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. See 5 U.S.C. 552a(i)(1). Furthermore, employees and contractors with access to databases maintaining PII must annually sign a sanction 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 record 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: 75 FR 79065, Repository of Electronic Authentication Data Master File. 83 FR 54969, Repository of Electronic Authentication Data Master File.

[FR Doc. 2023-04705 Filed: 3/7/2023 8:45 am; Publication Date: 3/8/2023]