SOCIAL SECURITY ADMINISTRATION

[Docket No. SSA-2018-0004]

Privacy Act of 1974; System of Records

AGENCY: Deputy Commissioner for Human Resources, Social Security Administration (SSA).

ACTION: Notice of a New System of Records

SUMMARY: In accordance with the Privacy Act, we are issuing public notice of our intent to establish a new system of records entitled, Security and Suitability Files (60-0377). This notice publishes details of the new system as set forth 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 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 5 U.S.C. 552a(e)(4) and (e)(11), the public is given 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-2018-0004. 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: Jasson Seiden, 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) 597-4307, e-mail: Jasson.Seiden@ssa.gov.

SUPPLEMENTARY INFORMATION: Persons appointed to, and under consideration for, Federal service or contract employment are required, with limited exceptions, to submit to a suitability background investigation. In addition, other individuals granted access to agency facilities and records may be required to complete such an investigation. The Deputy Commissioner for Human Resources, Office of Personnel, Center for Suitability and Personnel Security (CSPS) oversees and is responsible for adjudicating these investigations. Suitability and security related information that we collect during the investigations process and send to the Office of Personnel Management (OPM) is covered by OPM/Central-9, Personnel Investigations Records. The new Security and Suitability Files system of records covers suitability and security related information that we generate during the investigation process but that we do not send to OPM. We will use the information we collect to conduct background investigations for the

purpose of establishing that individuals employed by us, working under contract for us, or otherwise granted access to our facilities and records are suitable for such employment or access.

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

Dated: June 5, 2018.

Mary Ann Zimmerman,

Acting Executive Director,

Office of Privacy and Disclosure,

Office of the General Counsel.

Editorial note: This document was received for publication by the Office of the Federal Register on November 8, 2018.

SYSTEM NAME AND NUMBER: Security and Suitability Files, 60-0377

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION:

Social Security Administration

Deputy Commissioner for Human Resources

Office of Personnel

Center for Suitability and Personnel Security (CSPS)

6401 Security Boulevard

Baltimore, MD 21235; or the initiating regional office (See Appendix C for address information).

Office of Personnel Management

National Background Investigations Bureau (NBIB)

1137 Branchton Road, PO Box 618,

Boyers, PA 16018

Defense Information Systems Agency (DISA)

DISA Defense Enterprise Computing Center (DECC)

3990 E Broad Street

Columbus, OH 43213-1152

SYSTEM MANAGER(S):

Social Security Administration

Deputy Commissioner for Human Resources

Office of Personnel

Center for Suitability and Personnel Security (CSPS)

6401 Security Boulevard

Baltimore, MD 21235; or the initiating regional office (See Appendix C for address information).

csps.controls.response@ssa.gov

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Section 205(a) of the Social Security Act, as amended, HSPD-12 (Policy for a Common Identification Standard for Federal Employees and Contractors), Executive Orders 13764 (Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters) and 12968 (Access to Classified Information), Sections 3301 and 3302 of Title 5, U.S.C., and Parts 5, 731, 732, and 736 of Title 5 of the Code of Federal Regulations; and Fair Credit Reporting Act.

PURPOSE(S) OF THE SYSTEM: We will use the information in the Security and Suitability Files to determine the suitability of individuals for appointment or retention as an SSA employee, for access to SSA facilities and information systems, to hold sensitive positions, and to perform work or services for or on behalf of SSA as a contractor or volunteer. This will

ensure that all of our prospective, current, and former employees, students, contractors, grantees, appointees, cooperative agreement awardees, volunteers, and others granted access to our facilities and records are investigated appropriately for security and suitability, and that the results of the investigations when necessary, are adjudicated based on federal law and regulations and are recorded in the official records.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals seeking, or who have sought, to fill an available vacancy with SSA, or to otherwise be granted access to SSA facilities and records. This category of individuals include, but are not limited to, prospective, current, and former employees, students, contractors, grantees, appointees, cooperative agreement awardees, volunteers, and others who perform services for SSA.

CATEGORIES OF RECORDS IN THE SYSTEM: This system maintains information collected as part of our security and suitability investigative process. This information may include the individual's name, address, date of birth (DOB), Social Security number (SSN), phone number, driver's license information, fingerprints, residential and employment addresses, employment history (e.g., names of supervisors and colleagues), financial and educational background, professional experience information, and information from personal and professional references. We may also collect information about personal and professional conduct that could include disciplinary, criminal, and credit histories. This system may also include determinations of sensitivity and risk level for different positions and information to ensure compliance with security and suitability requirements, and information necessary to monitor and track security and suitability investigations for management workload purposes.

RECORD SOURCE CATEGORIES: We obtain information in this system primarily from the individuals to whom the record pertains. Information may also be obtained from, but not limited to references, credit reporting agencies, other federal agencies, and educational institutions.

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 Internal Revenue Service Code, unless authorized by statute, the Internal Revenue Service (IRS), or IRS regulations.

1. To the Office of the President in response to an inquiry from that office made on behalf of, and at the request of, the subject of the record or 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 his/her official capacity; or:

(c) any SSA employee in his/her 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 SSA determines the litigation is likely to affect SSA or any of its components,

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, the agency determines that disclosure of the records to DOJ, a court or other tribunal, or another party is a use of the information contained in the records that 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 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 the 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 SSA records in order to perform their assigned agency functions.

6. To the Equal Employment Opportunity Commission (EEOC or Commission) when requested in connection with investigations into alleged or possible discriminatory practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission.

7. To the Federal Labor Relations Authority, its General Counsel, the Federal Mediation and Conciliation Service, the Federal Service Impasses Panel, or an arbitrator when information is requested in connection with investigations of allegations of unfair practices, matters before an arbitrator or the Federal Service Impasses Panel.

8. To the Office of Personnel Management (OPM), the Merit Systems Protection Board, or the Office of Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigations of alleged or possible prohibited practices, and other such functions promulgated in 5 U.S.C. Chapter 12, or as may be required by law.

9. To Federal, State, and local law enforcement agencies and private security contractors, as appropriate, information necessary:
   (a) to enable them to protect the safety of SSA employees and customers, the security of the SSA workplace, and the operation of SSA facilities, or
   (b) to assist in investigations or prosecutions with respect to activities that affect such safety and security or activities that disrupt the operation of SSA facilities.

10. To the National Archives and Records Administration (NARA) under 44 U.S.C. 2904 and 2906.

11. To a Federal agency in response to its request, or at SSA's initiative, in connection with decisions to hire or retain an employee, issue a security clearance, conduct a security or suitability investigation, classify a job, award a contract, or regarding the requesting agency's decision to issue a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

12. To officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting conditions of employment.

13. 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 the 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 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.

14. To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

15. 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 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.

16. To the Department of Defense or other Federal agencies in connection with providing approved shared services to subscribing agencies for hiring or retaining an employee; classifying a position; conducting a security, suitability, fitness, or credentialing background investigation (including continuous evaluation/continuous vetting); issuing a security clearance or sensitive position eligibility; making a suitability, fitness, or credentialing decision; or recording the results of any agency decision with respect to these functions.

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

DISCLOSURE TO CONSUMER REPORTING AGENCIES: None.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: We will retrieve records in this system by name, SSN, and DOB.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records are temporary. We retain and destroy this information in accordance with the NARA approved General Records Schedules (GRS) 2.0, Human Resources, and GRS 5.6, Security Records. We retain investigative records on employees or applicants for employment, whether or not a security clearance is granted, and other persons, such as those performing work under contract or as volunteers in accordance with the approved records schedules. We retain investigative reports in accordance with OPM Central-9 (81 FR 70191) or successor Records Disposition Authority. Our shared service provider for tracking post-investigation data, the Department of Defense (DoD), retains post-investigative files and the computerized data bases in accordance with the Defense Manpower Data Center (DMDC) retention policies as published in DMDC 24 DoD (81 FR 39032) or successor Records Disposition Authority.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: We retain electronic and paper files with personal identifiers in secure storage areas accessible only by our authorized 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 number and password, and personal identification verification cards. We keep paper records in locked cabinets within secure areas, with access limited to only those employees who have an official need for access in order to perform their duties.

We annually provide our employees and contractors with appropriate security awareness training that includes reminders about the need to protect personally identifiable information (PII) and the criminal penalties that apply to unauthorized access to, or disclosure of, PII (5 U.S.C. 552a(i)(1)). Furthermore, employees and contractors with access to databases maintaining PII must sign a sanctions document annually, acknowledging their accountability for inappropriately accessing or disclosing such information.

The system is protected against compromise of PII and cyberattack by the full suite of defenses and sensors of the DoD cybersecurity perimeter. Data is encrypted where it is stored, and network traffic is encrypted based on the type of user traffic and risk to PII data. User access to data is protected using Identity and Access Management with multifactor authentication that will only allow an authenticated user to access and manipulate the specific records based on user role and permissions. The system audits access to information. Physical entry is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to the system must complete Information Assurance and Privacy Act training before initially accessing the system and annually thereafter, and these users must have also been through the information technology and/or security clearance eligibility process.

RECORD ACCESS PROCEDURES: This system of records has been exempted from the Privacy Act's access, contesting, and notification provisions as stated below. However, 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: This system of records has been exempted from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in today's Federal Register.

HISTORY: None.

[FR Doc. 2018-24853 Filed: 11/14/2018 8:45 am; Publication Date: 11/15/2018]