SYSTEM NUMBER: 60-0104

SYSTEM NAME:

Race and Ethnicity Collection System (RECS), Social Security Administration (SSA)

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

SSA, Office of Telecommunications and Systems Operations, 6401 Security Boulevard, Baltimore, Maryland 21235.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Successfully enumerated applicants for Social Security number (SSN) cards, other than those who receive cards through the enumeration-at-birth (EAB) or enumeration-at-entry programs (EAE), when such persons voluntarily provide race and ethnicity (RE) data.

CATEGORIES OF RECORDS IN THE SYSTEM:

SSN and RE data collected during contacts with the successfully enumerated applicants for SSN cards described above.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sections 702, 704 and 1106 of the Social Security Act (42 U.S.C. 902, 904, and 1306), and SSA regulations at 20 C.F.R. 401.165.

PURPOSE(S):

This system of records will cover RE data collected during contacts with persons who conduct enumeration business with us, other than those who receive cards through the EAB or EAE programs.

ROUTINE USES OF RECORDS COVERED BY THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Routine use disclosures are as indicated below:

1. To the Office of the President in response to an inquiry from that office made at the request of the subject of the record or a third party on that person's behalf.

2. To a congressional office in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf.

3. To the Department of Justice (DOJ), a court, other tribunal, or another party before such court or tribunal when:

    a) SSA or any of our components;

    b) Any SSA employee in his or her official capacity;

    c) Any SSA employee in his or her individual capacity when DOJ (or SSA when we are authorized to do so) has agreed to represent the employee; or

    d) The United States or any agency thereof when we determine that the litigation is likely to affect the operations of SSA or any of our components,
    is party to litigation or has an interest in such litigation, and we determine that the use of such records by DOJ, a court, other tribunal, or another party before such court or tribunal is relevant and necessary to the litigation. In each case, however, we must determine that such disclosure is compatible with the purpose for which we collected the records.

4. To a Federal, State, or congressional support agency (e.g., Congressional Budget Office and the Congressional Research Staff in the Library of Congress) for research, evaluation, or statistical studies. Such disclosures include, but are not limited to:

    a) Releasing information to assess the extent to which one can predict eligibility for Supplemental Security Income (SSI) payments or Social Security disability insurance benefits or other programs under the Social Security Act;

    b) Examining the distribution of benefits under programs of the Social Security Act by economic and demographic groups and how these differences might be affected by possible changes in policy;

    c) Analyzing the interaction of economic and non-economic variables affecting entry and exit events and duration in the Title II Old Age, Survivors, and Disability Insurance and the Title XVI SSI disability programs; and,

    d) Analyzing retirement decisions focusing on the role of Social Security benefit amounts, automatic benefit recomputation, the delayed retirement credit, and the retirement test. We may make these disclosures if we:

1) Determine that the routine use does not violate legal limitations under which the record was provided, collected, or obtained;
2) Determine that the purpose for which the proposed use is to be made:

i) Cannot reasonably be accomplished unless the record is provided in a form that identifies a person;
ii) Is of sufficient importance to warrant the effect on, or risk to, the privacy of the person which such limited additional exposure of the record might bring;
iii) Has a reasonable probability of being accomplished;
v.) Is of importance to the programs under the Social Security Act and beneficiaries of such programs or is for an epidemiological research project that relates to programs under the Social Security Act or beneficiaries of such programs;

5) Require the recipient of information to:

i) Establish appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record and agree to on-site inspection by our employees, our agents, or by independent agents of the recipient agency of those safeguards;
ii) Remove or destroy the information that enables the person to be identified at the earliest time that the recipient can do so consistent with the purpose of the project, unless the recipient receives written authorization from us that it is justified, based on research objectives, in retaining such information;
iii) Make no further use of the records except:

(a) under emergency circumstances affecting the health and safety of a person following written authorization from us;

(b) for disclosure to an identified person approved by us for the purpose of auditing the research project;

v) Keep the data as a system of statistical records. A statistical record is one which is maintained only for statistical and research purposes and which is not used to make any determination about a person;

6) Secure a written statement by the recipient of the information attesting to the recipient's understanding of, and willingness to abide by, these provisions.

7). To our contractors and grantees performing program evaluation, research, and statistical activities directly relating to this system of records, and to contractors or grantees for another Federal or State agency performing such activities.

8). To student volunteers, persons working under a personal services contract, and others who are not technically Federal employees, when they are performing work for us as authorized by law, and they need access to information in our records in order to perform their assigned agency duties.

9). To the General Services Administration and the National Archives Records Administration (NARA) under 44 U.S.C. 2904 and 2906, as amended by the NARA Act, information that is not restricted from disclosure by Federal law for their use in conducting records management studies.

10). To the appropriate Federal, State, and local agencies, entities, and persons when (1) we suspect or confirm that the security or confidentiality of information in this system of records has been compromised; (2) we determine that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or our other systems or programs that rely upon the compromised information; and (3) we determine that disclosing the information to such agencies, entities, and persons is necessary to assist in our efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. We will use this routine use to respond only to those incidents involving an unintentional release of our records.

11). To Federal, State, and local law enforcement agencies and private security contractors, as appropriate, information necessary:

a) To enable them to assure the safety of our employees and the public, the security of our workplace, and the operation of our facilities; or

b) To assist investigations or prosecutions with respect to activities that affect such safety and security or activities that disrupt the operation of our facilities.

12. 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.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

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

RETRIEVABILITY:

We will retrieve records by SSN.

ACCESSIBILITY:

Our researchers and statisticians prepare micro-data files about persons who are current, recently terminated, or potential recipients of benefits from Social Security and related programs for program evaluation, research, and statistical studies. When the product is in the form of micro-data, we make it available without personal identifiers to our other components and certain other agencies for data processing and data manipulation.

SAFEGUARDS:

We retain electronic and paper files with personal identifiers in secure storage areas accessible only to our authorized employees and contractors. We limit access to data with personal identifiers from this system to persons or organizations authorized by our Office of Research, Evaluation, and Statistics. We furnish specially edited micro-files on request to public and private organizations for purposes of research and analysis. We include further confidentiality protections in our data agreements.

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

RETENTION AND DISPOSAL:

For purposes of records management disposition authority, we will follow the NARA and Department of Defense (DOD) 5015.2 regulations (DOD Design Criteria Standard for Electronic Records Management Software Applications). We will permanently maintain RE data covered by the RECS system of records. We will retain the research and statistical micro-data extract (stored on the mainframe) for a maximum of 100 years.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Enumeration and Death Alerts, Office of Earnings, Enumeration, and Administrative Systems, Social Security Administration, 6401 Security Boulevard, Baltimore, MD 21235.

NOTIFICATION PROCEDURES:

Persons can determine if this system contains a record about them by writing to the system manager at the above address and providing their name, SSN, or other information that may be in this system of records that will identify them. Persons requesting notification of records in person should provide the same information, as well as provide an identity document, preferably with a photograph, such as a driver's license or some other means of identification, such as voter registration card, etc. Persons lacking identification documents sufficient to establish their identity must certify in writing that they are the person they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another person under false pretenses is a criminal offense.

Persons requesting notification by telephone must verify their identity by providing identifying information that parallels the information in the record to which notification is being requested. If we determine that the identifying information the person provides by telephone is insufficient, the person will be required to submit a request in writing or in person. If a person requests information by telephone on behalf of another individual, the subject person must be on the telephone with the requesting person and with us in the same phone call. We will establish the subject person's identity (his or her name, SSN, address, date of birth, and place of birth, along with one other piece of information such as mother's maiden name), and ask for his or her consent to provide information to the requesting person.

Persons requesting notification submitted by mail must include a notarized statement to us to verify their identity or must certify in the request that they are the person they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another person under false pretenses is a criminal offense. These procedures are in accordance with SSA Regulations (20 C.F.R. 401.40).

RECORD ACCESS PROCEDURES:

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. These procedures are in accordance with SSA Regulations (20 C.F.R. 401.40(c)).

CONTESTING RECORD PROCEDURES:

Same as notification procedures. Requesters 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 SSA Regulations (20 C.F.R. 401.65(a)).

RECORD SOURCE CATEGORIES:

We obtain information covered by this system of records from successfully enumerated applicants for original or replacement SSN cards (or from third parties acting on their behalf) who are not enumerated through the EAB or EAE programs.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.