Social Security Administration

Privacy Act of 1974, as Amended

Proposed System of Records and Routine Use Disclosures

AGENCY: Social Security Administration (SSA)

ACTION: Proposed System of Records and Routine Uses

SUMMARY: In accordance with the Privacy Act (5 U.S.C. § 552a(e)(4) and (e)(11)), we are issuing public notice of our intent to establish a system of records, the *Central Repository of Electronic Authentication Data Master File* (hereinafter referred to as the *e-Authentication File*) and its applicable routine uses. The *e-Authentication File* will maintain personally identifiable information (PII) we collect and use to verify the identity of persons using our electronic services. We discuss the *e-Authentication File* and its routine use disclosures in the Supplementary Information section below. We invite public comments on the *e-Authentication File*.

DATES: We filed a report of the *e-Authentication File* and its applicable routine use disclosures with the Chairman of the Senate Committee on Homeland Security and Governmental Affairs, the Chairman of the House Committee on Oversight and Government Reform, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on November 30, 2010. The *e-Authentication File* and applicable routine uses will become effective on January 13, 2010, unless we receive comments before that date that require further consideration.

ADDRESSES: Interested persons may comment on this publication by writing to the Executive Director, Office of Privacy and Disclosure, Office of the General Counsel, Social Security Administration, 3-A-6 Operations Building, 6401 Security Boulevard, Baltimore, Maryland 21235-6401 or through the Federal e-Rulemaking Portal at http://www.regulations.gov. 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: Neil Etter, Social Insurance Specialist, Disclosure Policy Development and Services Division I, Office of Privacy and Disclosure, Office of the General Counsel, Social Security Administration, 3-A-6 Operations Building, 6401 Security Boulevard, Baltimore, Maryland 21235-6401, telephone: (410) 965-8028, email: neil.etter@ssa.gov.

SUPPLEMENTARY INFORMATION:

I. Background and Purpose of the *e-Authentication File*

A. General Background

We provide electronic services, such as our automated telephone and Internet applications, to persons doing business with us. When users choose our electronic services, they must provide their PII. We use their PII to verify their identities. Upon successful verification, we are able to recognize the users' identities and authorize them to conduct business with us electronically.

The *e-Authentication File* supports our agency's objectives to expand electronic services and to provide strong and secure authentication procedures. For security reasons, we must be able to determine, with confidence, persons are who they claim to be each time they choose our electronic services. The *e-Authentication File* will capture the data we need to verify users' identities.

B. Collection and Maintenance of the Data Covered by the *e-Authentication File*

We will collect and maintain the users' PII in the *e-Authentication File*. The PII may include the user's name, address, date of birth, Social Security number (SSN), phone number, and other types of identifying information (e.g., address information of persons from the W-2 and Schedule Self Employed (SE) forms we receive electronically for our programmatic purposes, as permitted by 26 U.S.C. § 6103(l)(1)(A)). We may also collect knowledge-based authentication data, which is information users establish with us or that we already maintain in existing Privacy Act systems of records.

We will keep the data necessary to administer and maintain our e-Authentication infrastructure. This includes management and profile information, such as blocked accounts, failed access data, effective date of passwords, and other data that allows us to evaluate the system's effectiveness. The data we maintain also may include archived transaction data and historical data.

II. Routine Use Disclosures of Data Covered by the *e-Authentication File*

A. Routine Use Disclosures

We propose to establish the following routine use disclosures of information from the *e-Authentication File:*

1. ***To the Office of the President in response to a request the Office of the President made at the request of the subject of a record or a third party acting on the subject's behalf.***

   We will disclose information under this routine use only when the Office of the President indicates it is requesting the record on behalf of the subject of the record or a third party acting on the subject's behalf.

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

   We will disclose information under this routine use only when a Member of Congress, or member of his or her staff, indicates he or she is requesting the record on behalf 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 a court or other tribunal when:***

a) SSA or any of our components; or

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

c) any SSA employee in his or her individual capacity when DOJ (or SSA) 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 a 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 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.

We will disclose information under this routine use as necessary to enable the DOJ to defend us, our components, or our employees, in litigation when we determine the use of information covered by the *e-Authentication File* is relevant and necessary to the litigation and compatible with the purpose for which we collected the information. We will also disclose information to ensure that courts, other tribunals, and parties before such courts or tribunals, have appropriate information that we determine is relevant and necessary.

4. ***To other Federal agencies and our contractors, including external data sources, to assist us in efficiently administering our programs.***

We will disclose information under this routine use only in situations where we have a contractual agreement or similar agreement with a third party to assist in accomplishing our work relating to information covered by the *e-Authentication File*. Under this routine use, we may disclose information to a contractor to assist us in advancing, testing, and evaluating our authentication procedures for our electronic services.

5. ***To student volunteers, persons working under a personal services contract, and others when they need access to information in our records in order to perform their assigned agency duties.***

We will disclose information under this routine use only when we use the services of student volunteers, persons working under a personal services contract, and others in educational, training, employment, and community service programs, when they need access to information covered by the *e-Authentication File* to perform their assigned agency duties.

6. ***To the Department of Justice for:***

a) investigating and prosecuting violations of the Social Security Act to which criminal penalties attach; and

b) representing the Commissioner; or

c) investigating issues of fraud or violation of civil rights by agency officers or employees.

We will disclose information under this routine use only as necessary to enable DOJ to represent us in matters for these purposes.

7. ***To the General Services Administration (GSA) and the National Archives and Records Administration (NARA) under 44 U.S.C. §§ 2904 and 2906, as amended by the NARA Act of 1984, when the information is for records management purposes.***

We will disclose information under this routine use only when it is necessary for GSA and NARA to have access to the information covered by the *e-Authentication File*. The Administrator of GSA and the Archivist of NARA are authorized by Title 44 U.S.C. § 2904, as amended, to promulgate standards, procedures, and guidelines regarding records management, and to conduct records management studies. Title 44 U.S.C. § 2906, as amended, provides that agencies are to cooperate with GSA and NARA as GSA and NARA are authorized to inspect Federal agencies' records for records management purposes.

8. ***To appropriate Federal, State, and local agencies, entities, and persons when:***

a) we suspect or confirm a compromise of security or confidentiality of information;

b) we determine that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property

interests, risk of identity theft or fraud, or risk of harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and

c) we determine that disclosing the information to such agencies, entities, and persons will assist us in our efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy any harm.

We will disclose information under this routine use specifically in connection with response and remediation efforts in the event of an unintentional release of agency information (otherwise known as a data breach). With this routine use, we can protect the interests of the people whose information is at risk by responding timely and effectively to a data breach. The routine use will also help us improve our ability to prevent, minimize, or remedy any harm that may result from a data breach.

B. Compatibility of Routine Uses

We can disclose information for routine uses one through six when it is necessary to carry out our programs or other programs similar to ours or when the disclosure is supported by a published routine use (20 C.F.R. § 401.150). We can also disclose information when the disclosure is required by law (20 C.F.R. § 401.120). Federal law requires the disclosures that we make under routine uses seven and eight, to the extent another Federal law does not prohibit the disclosure. All routine uses in the

e-Authentication File are compatible with the relevant statutory and regulatory criteria.

III. Records Storage Medium and Safeguards for the Information Covered by the *e-Authentication File*

We will maintain, in electronic form, all information covered by the *e-Authentication File*. We will safeguard the security of the electronic information covered by the *e-Authentication File* by requiring the use of access codes (personal identification number (PIN) and password) to enter the computer system that will house the data. We will maintain audit trails of all access to this information in accordance with agency security policy and Federal retention standards. We will permit access to the information covered by the *e-Authentication File* only to our authorized employees and contractors who require the information to perform their official duties.

We annually provide all our employees and contractors with security awareness and training. This training includes the need to protect PII and the criminal penalties that apply to an unauthorized access to, or disclosure of, PII. Employees and contractors with access to databases maintaining PII must also sign a sanction document annually, acknowledging their accountability for inappropriately accessing or disclosing such information.

IV. Effects of the *e-Authentication File* on the Rights of Persons

We will use safeguards to protect the confidentiality of all PII in our possession. We will ensure that all contractors or others acting on our behalf are obliged to do the same. We will adhere to the provisions of the Privacy Act and other applicable Federal statutes that govern our use and disclosure of information that the *e-Authentication File* covers. We will disclose information under the routine uses only as necessary to accomplish the stated purposes. We do not anticipate that the *e-Authentication File,* or its applicable routine use disclosures, will have any unwarranted adverse effect on the privacy or other rights of persons.

DATED: November 30, 2010

/s/
Michael J. Astrue
Commissioner

Social Security Administration

Notice of System of Records

Required by the Privacy Act of 1974, as Amended

System number: 60-0373

System name: *Central Repository of Electronic Authentication Data Master File*

Security classification: None

System Location: Social Security Administration (SSA), Office of Systems, 6401 Security Boulevard, Baltimore, Maryland 21235.

Categories of persons covered by the system: Persons conducting business with us through our electronic services.

Categories of records in the system: We will collect and maintain the user's personally identifiable information (PII) in this system of records. The PII may include the user's name, address, date of birth, Social Security number (SSN), phone number, and other types of identity information (e.g., address information of persons from the W-2 and Schedule Self Employed (SE) forms we receive electronically for our programmatic purposes as permitted by 26 U.S.C. § 6103(l)(1)(A)). We may also collect knowledge-based authentication data, which is information users establish with us or that we already maintain in existing Privacy Act systems of records. We will maintain the data necessary to administer and maintain our e-Authentication infrastructure. This includes management and profile information, such as blocked accounts,

failed access data, effective date of passwords, and other data that allows us to evaluate the system's effectiveness. The data we maintain also may include archived transaction data and historical data.

Authority for maintenance of the system: Section 205(a) of the Social Security Act; the Government Paperwork Elimination Act (P.L. 105-277); the Internal Revenue Code (26 U.S.C. § 6103(l)(1)(A)); and the Federal Information Security Management Act of 2002 (Title III) of the E-Government Act of 2002 (P.L. 107-347).

Purpose(s): This system of records supports our agency's objectives to expand electronic services, such as our automated telephone and Internet application. This system of records also supports our agency's commitment to strong and secure authentication procedures by properly maintaining PII we collect from persons to verify their identities. For security reasons, we must be able to determine, with confidence, persons are who they claim to be each time they choose our electronic services.

Routine uses of records covered by this system of records, including categories of users and the purposes of such uses: Routine use disclosures are indicated below; however, we will not disclose any information defined as "return or return information" under 26 U.S.C. § 6103 of the Internal Revenue Code (IRC), unless the IRC, the Internal Revenue Service (IRS), or IRS regulations authorize us to do so.

1. ***To the Office of the President in response to a request the Office of the President made at the request of the subject of the record or a third party acting on the subject's behalf.***

2. ***To a congressional office in response to a request from that office made 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, other tribunal, or another party before such court or tribunal when:***

   a) SSA or any of our components; or

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

   c) any SSA employee in his or her individual capacity when DOJ (or SSA) 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 a 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 tribunal, is relevant and necessary to the litigation. In each case, we must determine that such disclosures are compatible with the purpose for which we collected the records.

4. ***To other Federal agencies and our contractors, including external data sources, to assist us in administering our programs.***

5. ***To student volunteers, persons working under a personal services contract, and others when they need access to information in our records in order to perform their assigned agency duties.***

6. ***To the Department of Justice for:***
   a) ***investigating and prosecuting violations of the Social Security Act to which criminal penalties attach; and***
   b) ***representing the Commissioner; or***
   c) ***investigating issues of fraud or violation of civil rights by agency officers or employees.***

7. ***To the General Services Administration and the National Archives and Records Administration under 44 U.S.C. §§ 2904 and 2906, as amended by the NARA Act of 1984, when the information is for records management purposes.***

8. ***To appropriate Federal, State, and local agencies, entities, and persons when:***
   a) ***we suspect or confirm a compromise of security or confidentiality of information;***
   b) ***we determine that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, risk of identity theft or fraud, or harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and***
   c) ***we determine that disclosing the information to such agencies, entities, and persons will assist us in our efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.***

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in this system of records:

Storage: We will store records in this system of records in electronic form.

Retrievability: We will retrieve records in this system of records by a person's name and associated identifying information.

Safeguards: We retain electronic files with personal identifiers in secure storage areas accessible only to our authorized employees and contractors who have a need for the information when performing their official duties. Security measures include the use of access codes (personal identification number (PIN) and password) to enter our computer systems that house the data.

We annually provide all our employees and contractors with security awareness and training. This training includes the need to protect PII and the criminal penalties that apply to an unauthorized access to, or disclosure of, PII. Employees and contractors with access to databases maintaining PII must also sign a sanction document annually, acknowledging their accountability for inappropriately accessing or disclosing such information.

Retention and disposal: We maintain records in SSA headquarters within the Office of Open Government. We will maintain records in this system of records until seven years after the notification of the death of the account holder. After that time, we will delete the person's records from the database.

System manager(s) and address: Office of the Chief Information Officer, Office of Open Government, 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 in this system of records that will identify them. Persons requesting notification 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.

Persons requesting notification of records in person must provide the same information, as well as provide an identity document, preferably with a photograph, such as a driver's license. 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 about which they are requesting notification. If we determine that the identifying information the person provides by telephone is insufficient, we will require the person to submit a request in writing or in person. If a person requests information by telephone on behalf of another person, the subject person must be on the telephone with the requesting person and 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. These procedures are in accordance with our regulations at 20 C.F.R. §§ 401.40 and 401.45.

Record access procedures: Same as notification procedures. Persons also should reasonably specify the record contents they are seeking. These procedures are in accordance with our regulations (20 C.F.R. § 401.40(c)).

Contesting record procedures: Same as notification procedures. Persons also should 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 (20 C.F.R. § 401.65(a)).

Record source categories: We obtain information in this system of records primarily from the person to whom the record pertains. We may also include information from electronic W-2 and electronic Schedule SE forms for members of the public.

System exempted from certain provisions of the Privacy Act: None.