

**Supporting Statement for  
Social Security Administration's Public Credentialing and  
Authentication Process  
20 CFR 401.45, 20 CFR 402  
OMB No. 0960-0789**

**A. Justification**

**1. Introduction/Authoring Laws and Regulations**

The Social Security Administration (SSA) is continuing its public credentialing and authentication process that provides secure access to SSA's electronic services.

With this continued process, we offer consistent authentication across SSA's secured online services. We allow our users to request and maintain only one User ID, consisting of a self-selected Username and Password, to access multiple Social Security electronic services. Designed in accordance with the Office of Management and Budget (OMB) Memorandum M-04-04 and the National Institute of Standards and Technology (NIST) Special Publication 800-63, this process provides the means of authenticating users of our secured electronic services and streamlines access to those services.

SSA's public credentialing and authentication process:

- Issues a single User ID to anyone who wants to do business with the agency;
- Offers authentication options that meet the changing needs of the public;
- Partners with an external data service provider to help us verify the identity of our online customers;
- Complies with relevant standards;
- Offers access to some of SSA's heaviest, but more sensitive, workloads online while providing a high level of confidence in the identity of the person requesting access to these services;
- Offers an in-person process for those who are uncomfortable with, or unable to use, the Internet process;
- Balances security with ease of use; and
- Provides a user-friendly way for the public to conduct extended business with us online instead of visiting local servicing offices or requesting information over the phone. Individuals have real-time access to their Social Security information in a safe and secure web environment.

**2. Description of Collection**

We collect and maintain the users' personally identifiable information (PII) in our *Central Repository of Electronic Authentication Data Master File* Privacy Act system of records which we published in the Federal Register (December 17, 2010, at 75 FR 79065). The PII may include the users' name, address, date of birth, Social Security number, phone number, and other types of identity information [e.g., address information of persons from the W-2 and Schedule Self Employed 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 our existing Privacy Act systems of records.

We retain 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.

We collect, maintain, and distribute confidential and non-confidential information in accordance with *42 U.S.C. 1306*, *20 CFR 401* and *402*, *5 U.S.C. 552* (Freedom of Information Act), *5 U.S.C. 552a* (Privacy Act of 1974, as amended), Internal Revenue Code (*26 U.S.C. § 6103(l)(1)(A)*), Federal Information Security Management Act of 2002 (*Title III*) of the E-Government Act of 2002 (*Pub.L. 107-347*, section 301), and OMB Circular No. A-130.

We use the information from this collection to identity proof and authenticate our users online and to allow them access to their personal information from our records. We also use this information to provide second factor authentication. We are committed to expanding and improving this process so we can grant access to additional online services in the future.

Offering online services is not only an important part of meeting SSA's goals, but is vital to good public service. In increasing numbers, the public expects to conduct complex business over the Internet. Ensuring SSA's online services are both secure and user-friendly is our priority. With the limited data we have, it is difficult for SSA to meet the OMB and NIST authentication guidelines for identity proofing the public. Therefore, we awarded a competitively bid contract to an external data service provider, Experian<sup>1</sup>, to help us verify the identity of our online customers. We use this External Data Service (EDS), in addition to our other authentication methods, to help us prove, or verify, the identity of our customers when they are completing online, electronic transactions with us.

### **Social Security's Authentication Strategy**

We remain committed to enhancing our online services using authentication processes which balance usability and security. We continue to research and develop new authentication tools while monitoring the emerging threats.

The following are key components of our authentication strategy:

- **Enrollment and Identity Verification** – We collect identifying data and use SSA and EDS records to verify an individual's identity. Individuals have the option of obtaining an enhanced, stronger, User ID by providing certain financial information (e.g., Medicare wages, self-employed earnings, direct deposit amount, or the last eight digits of a credit card number) for verification. We also

---

<sup>1</sup> Experian is a global information services company. Experian's decisional solutions enable Social Security to manage and optimize risk as well as prevent, detect, and reduce fraud.

ask individuals to answer out-of-wallet questions so we can further verify their identities. Individuals who are unable to complete the process online can present identification at a field office to obtain a User ID.

- **Establishing the User Profile** – The individual self-selects a username and password, both of which can be of variable length and alphanumeric. We provide a password strength indicator to help the individual select a strong password. We also ask the individual to choose challenge questions for use in restoring a lost or forgotten username or password.
- **Enhancing the User ID** – If an individual opts to enhance or upgrade the User IDs, we mail a one-time-use upgrade code to the individual’s verified residential address. When the individual receives the upgrade code in the mail, he or she can enter this code online to enhance the security of the account. At this time, we also ask the individual to enter a cell phone number. We send an initial text message to that number and require the individual to confirm its receipt. We send a text message to that number each time the individual signs in, subsequently.
- **Login and Use** – Standard authentication provides an individual with a User ID for access to most online applications. Enhanced authentication uses the standard User ID along with a one-time code sent to the individual’s cell phone, via text message, to create a more secure session, and to grant access to certain sensitive Social Security services. An individual who forgets the password can reset it automatically without contacting SSA.

The enrollment process is a one-time only activity for the respondents. After the respondents enroll and choose their User ID (Username & Password), they have to sign in with their User ID every time they want to access Social Security’s secured online services.

SSA requires individuals to agree to the “Terms of Service” detailed on our web site before we allow them to begin the enrollment process. The “Terms of Service” inform the individuals what we will and will not do with their personal information and the privacy and security protections we provide on all data we collect. These terms also detail the consequences of misusing this service.

In order to verify an individual’s identity, we ask the individual to give us minimal personal information, which may include:

- Name;
- Social Security Number;
- Date of birth;
- Address – mailing and residential;
- Telephone number;
- E-mail address;
- Financial information;
- Cell phone number; and

- Selecting and answering password reset questions.

We send a subset of this information to the EDS, who then generates a series of out-of-wallet questions back to the individual. The individual must answer all or most of the questions correctly before continuing in the process. The exact questions generated are unique to each individual.

This collection of information, or a subset of it, is mandatory for respondents who want to do business with SSA via the Internet. We collect this information via the Internet, on SSA's public-facing website. We also offer an in-person identification verification process for individuals who cannot, or are not willing, to register online. For the in-person process, the individual must go to a local SSA field office and provide identifying information. We do not ask for financial information with the in-person process.

We only collect the identity verification information one time, when the individual registers for a credential. We ask for the User ID (Username and password) every time an individual signs in to our automated services. If individuals opt for the enhanced or upgraded account, they also receive a text message on their cell phones (this serves as the second factor for authentication) each time they sign in.

### **3. Use of Information Technology to Collect the Information**

We collect this information electronically via the Internet through SSA's public-facing website: [www.socialsecurity.gov](http://www.socialsecurity.gov), under the agency's Government Paperwork Elimination Act plan. We also collect this information through an in-person process for those who cannot, or choose not to, complete the registration online. For the in-person process, the individual provides the information to an SSA representative during a field office interview. The representative enters the information via an Intranet customer service application. Approximately 25 percent of respondents use the in-person process to register for a User ID. Approximately 75 percent of respondents use the online process.

### **4. Why We Cannot Use Duplicate Information**

The nature of the information we are collecting and the manner in which we are collecting it would normally preclude duplication. Although we currently use other collection instruments to obtain similar data, this identity verification, public credentialing, and authentication process offers the public additional features the applications noted below do not, for example, enhanced identity verification, access to multiple Social Security electronic services, and enhancement or upgrade of User IDs.

- RISA – Request for Internet and Automated 800# Services – Knowledge-Based Authentication for the Individual, OMB #0960-0596
- IRES – Single Sign-On (SSO) & Integrated Registration Services for Business Services Online (BSO), OMB #0960-0626

Further, this identity verification, public credentialing, and authentication process will eventually absorb and replace the existing collections (mentioned above). We plan to

accomplish this work through a series of annual releases. Additional releases will reduce the burden of the existing collections. We will prepare change requests for the existing collections to adjust the burden as needed.

**5. Minimizing Burden on Small Respondents**

This collection does not affect small businesses or other small entities.

**6. Consequence of Not Collecting Information or Collecting it Less Frequently**

Failure to collect this information to verify an individual's identity would result in SSA's non-compliance with OMB & NIST guidelines (*OMB 04-04 & NIST SP 800-63*). In addition, failure in our ability to verify the requesters' identity would result in our inability to respond to their requests. Making this service available electronically saves the requester the effort of phoning a Social Security TeleService Center representative or visiting a Social Security field office, and it saves our staff time. We only collect this information on an as-needed basis; therefore we cannot collect it less frequently. There are no technical or legal obstacles that prevent burden reduction.

**7. Special Circumstances**

There are no special circumstances that would cause Social Security to conduct this information collection in a manner inconsistent with *5 CFR 1320.5*.

**8. Solicitation of Public Comment and Other Consultations with the Public**

The 60-day advance Federal Register Notice published on April 16, 2014 at 21496, and SSA received no public comments. The second Notice published on July 2, 2014, at 37828. If SSA receives any comments in response to the 30-day Notice, we will forward them to OMB.

We will continue to conduct focus group and usability testing with members of the public, both beneficiaries and non-beneficiaries, as we build upon and enhance this process.

**9. Payment or Gifts to Respondents**

Social Security does not provide payments or gifts to the respondents.

**10. Assurances of Confidentiality**

We can make disclosures without individual authorization only for purposes stated at the time of data collection (purposes typically identified in a system of records' routine use provisions), or specifically consented to thereafter by each of the parties to whom we provided the promise of confidentiality. SSA collects, maintains, and distributes confidential and non-confidential information in accordance with *42 U.S.C. 1306, 20 CFR 401 and 402, 5 U.S.C. 552* (Freedom of Information Act), *5 U.S.C. 552a* (Privacy Act of 1974), Internal Revenue Code (*26 U.S.C. 6103(l)(1)(A)*), *Federal Information Security Management Act of 2002 (Title III)* of the E-Government Act of 2002 (*P.L. 107-347*), and OMB Circular No. A-130.

**11. Justification for Sensitive Questions**

We ask questions of a sensitive nature in this Information Collection. We ask the responder some knowledge-based, “out-of-wallet” questions, and we ask the responder some “shared secret” questions. We may ask the responder for financial information. Before we ask for any information, the responders must read, and agree to our “Terms of Service,” which serves to acknowledge and indicate their consent to provide us with sensitive information. The “Terms of Service” explain what we will, and will not do with the information; it describes the responder’s responsibilities; and it explains SSA’s legal authority for collecting the information.

### **Out-of-Wallet Questions**

The EDS incorporates both public and private data to allow generation and evaluation of questions uniquely pertaining to a given consumer. We call these “out-of-wallet” questions. The EDS designs these questions so only the individual would know the answer. If someone stole the consumer’s wallet, the identity thief should not be able to answer these questions.

The categories of questions are as follows:

- 1) **Credit questions** – These questions incorporate information from the Credit Report of a consumer. The types of questions in the group are about specific lenders, dates, and terms of loans.
- 2) **Non-credit questions** – These are questions derived from various public and private databases. The types of questions in this group vary from automobile related questions, to questions on previous residences, to questions on professions or licenses, etc.

These questions are important because we use them to protect and verify an individual’s identity. We must ensure only the true individuals can access their personal information. We ask these questions only once, and in multiple-choice format, when the respondent enrolls to create an account with SSA. (See the screen package in Attachment A for examples of these questions.)

SSA does not have access to the information the individual provides to the EDS. SSA does not retain or have access to any of the information – questions and answers – after the transaction takes place.

### **Financial Information**

We may ask the individual to provide financial account information. If individuals want extra security, we ask them to provide financial account information in the form of W-2 information, self-employment information from tax returns, direct deposit information, or the last eight digits of a credit card; however, they can enroll for a standard account without providing it. We confirm financial account information as another way of ensuring an individual’s identity, either using our own records or, in the case of the last eight digits of a credit card, using the EDS’s records. The information the individuals provide does not allow us to access or view their financial accounts or credit records.

Providing this information is optional. We only ask for financial information one time, when the respondent enrolls to create a Social Security account with extra security. If the individuals are uncomfortable about giving us financial account information, they can still sign up for an account by visiting their local Social Security field office in person. We do not require financial information as part of the in-person process.

**Shared Secrets**

We collect shared secrets from the individuals to use as password reset questions to improve customer service and reduce workloads and costs. If the individuals lose or forget their password, we ask the three questions we established with the individuals during account setup when they originally created the User ID. The individuals must provide correct answers, consistent with the answers on record, to all three questions.

During registration, we ask the individuals to select and answer three password reset questions. We grouped these questions into three sets dealing loosely with persons, places, and things. The individuals must select one question from each of the following categories:

- Relationship questions;
- Geographic questions; and
- Objective questions.

Once the individuals provide correct answers to their shared secrets questions, the system will allow them to reset their password.

**12. Estimates of Public Reporting Burden**

We estimate that 38,251,877 respondents use the Internet process annually to create and manage an account with SSA and then authenticate to gain access to our secured online services. We estimate that it takes an average of 8 minutes to complete a transaction, resulting in an annual reporting burden of 5,100,250 hours. We calculated a separate cost burden for this process (see #13 below).

We estimate that 1,370,633 respondents use the Intranet process annually to create and manage an account with us. We estimate that it takes an average of 8 minutes to complete this transaction, resulting in an annual reporting burden of 182,751 hours. We did not calculate a separate cost burden for this process.

We use different modalities to collect the information, via the Internet and the Intranet. We included an estimated number of registrations and sign-ins when we calculated the total number of annual respondents. We included the number of additional annual registrations we anticipate due to the new services we are adding (as discussed in the Addendum). We estimated the number of minutes for completion by averaging the “time-on-task” figures we obtained from our usability testing. See chart below with the updated figures:

Modality of	Number of	Frequency	Average	Total Annual
-------------	-----------	-----------	---------	--------------

<b>Completion</b>	<b>Respondents</b>	<b>of Response</b>	<b>Burden Per Response (minutes)</b>	<b>Burden Hours (hours)</b>
Internet Respondents	38,251,877	1	8	5,100,250
Intranet Respondents	1,370,633	1	8	182,751
<b>Totals:</b>	<b>39,622,510</b>			<b>5,283,001</b>

The total annual burden for this information collection is **5,283,001** hours. This figure represents burden hours, and we calculated a separate cost burden for the respondents using the Internet process (see #13 below for details).

**13. Annual Cost to the Respondents**

There is no cost burden to the Intranet respondents. However, for the Internet respondents, there may be some cost if the respondent chooses extra security, since this is an optional service. Each time the respondents who request extra security log in to access SSA’s secured online services, we send a text message to their cell phone, including a code which they must then enter on the web page. We estimate approximately 2.6% of all respondents use the extra security feature (this includes the 2000 respondents who we expect to use this feature as part of the new iTOPSS service mentioned in the Addendum).

**Storage Management Subsystem (SMS) cost** -- code sent via text message from SMS to the individual user.

- For the user who receives the SMS code and does not have a text plan: the current cost could range from 10 cents to 20 cents per message.
- For the user who has a limited text plan: the cost would just be included as part of the plan. We have no way to estimate this cost.
- For the user who has an unlimited text plan, there would be no charge. The user would have paid for this service as part of the plan. We have no way to estimate cost.

Based on our current data, we estimate the respondents who use this service access the extra security feature approximately 167,500 times annually. Since we have no way to gauge the type of text plan these respondents use, we estimated the cost based on the full number of accessed features (167,500) costing an average of 15 cents each, for a total of \$25,125 annually.

**14. Annual Cost to Federal Government**  
**EDS Costs**

A key component of SSA’s registration and authentication process, which manifests itself as both an Internet application and an Intranet application, is the partnership with an EDS for the verification of personal information. SSA pays the EDS for expenses incurred via two tasks: a development and maintenance task and a transaction task. For FY 2013,



development and maintenance costs were \$1,100,000; and transaction costs (for both Internet and Intranet) were \$6,000,000; totaling \$7,100,000. For FY 2014, we estimate development and maintenance costs will be \$1,730,000; and transaction costs will be \$7,200,000; totaling \$8,930,000. The cost per transaction is 48 cents.

#### **Social Security Costs**

Social Security's internal cost to maintain this process is approximately \$860,000 per year.

#### **Total Social Security & EDS Costs**

The total FY 2013 cost to the Federal Government was approximately \$7,960,000. The total FY 2014 cost to the Federal Government will be approximately \$9,790,000.

#### **15. Program Changes or Adjustments to the Information Collection Request**

The burden increase is due to the inclusion of the new applications described in the Addendum. The burden has also increased as more people register for a credential and use it to come online to do business with us. In addition, as fewer people use our interview process, and more use the Internet process to register, we increased the burden for the Internet version and decreased it for the Intranet version.

Eventually, this identity verification, public credentialing, and authentication process will absorb and replace the existing authentication collections under OMB Control Numbers 0960-0596 and 0960-0626. (OMB Control Number 0960-0632 was decommissioned last year). We plan to accomplish this work through a series of annual releases. The future releases will reduce the burdens in the other existing authentication collections. SSA will continue to prepare change requests for the other existing authentication collections, as needed.

#### **16. Plans for Publication Information Collection Results**

SSA will not publish the results of the information collection.

#### **17. Displaying the OMB Approval Expiration Date**

SSA is not requesting an exception to the requirement to display the OMB approval expiration date.

#### **18. Exceptions to Certification Statement**

SSA is not requesting an exception to the certification requirements at 5 *CFR* 1320.9 and related provisions at 5 *CFR* 1320.8(b)(3).

#### **B. Collections of Information Employing Statistical Methods**

Social Security does not use statistical methods for this information collection.