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

## A. Justification

### 1. Introduction/Authoring Laws and Regulations

The Social Security Administration (SSA) is introducing a stronger citizen authentication process that will enable a new user experience and access to more electronic services. Authentication is the foundation for secure, online transactions. Identity authentication is the process of determining, with confidence, that someone is who he or she claims to be during a remote, automated session. It is comprised of three distinct factors: something you know (e.g., password), something you have (e.g., Federal identification {ID} badge), and something you are (e.g., fingerprint). Single-factor authentication uses one of the factors, and multi-factor authentication uses two or more of the factors.

With this new process, we are working towards offering consistent authentication across SSA's secured online services, and eventually, SSA's automated telephone services. We will allow our users to 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 new process provides the means of authenticating users of SSA's secured electronic services and streamlines access to those services.

SSA's new authentication strategy will:

- Issue a single User ID to anyone who wants to do business with the agency;
- Offer a variety of authentication options that meet the changing needs of the public;
- Partner with an external data service provider to help us verify the identity of our online customers;
- Comply with relevant standards;
- Offer 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;
- Offer an in-person process for those who are uncomfortable with or unable to use the Internet process; and
- Balance security with ease of use.

This new authentication strategy will provide 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 will have real time access to their Social Security information in a safe and secure web environment.

SSA collects this information by authority of the *Privacy Act of 1974* at *5 U.S.C. 552a(e)(10),*which requires agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. Also, *5 U.S.C. 552a(f)(2)&(3)* requires agencies to establish requirements for identifying an individual who requests a record or information pertaining to that individual and to establish procedures for disclosure of personal information. SSA promulgated Privacy Act rules in the *Code of Federal Regulations,* subpart *B.* Procedures for verifying identity are at *20 CFR 401.45.* Authority to collect this information is also contained in section *205(a)* of the *Social Security Act.*

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* (*Pub.L. 107-347,* section *301*), and OMB Circular No. A-130.

This is a new Information Collection Request for SSA's new identity verification, public credentialing, and authentication process.

**2. Description of Collection**

SSA will use the information from this collection to authenticate users and allow them to access and take action on their Social Security records. We are committed to expanding and improving our online applications. Our online applications have been indispensible in helping us keep up with the enormous growth in retirement claims. For that reason, we are exploring the expansion of our online applications to other key workloads.

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 that 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 have awarded a competitively bid contract to an external data service provider, Experian[1], to help us verify the identity of our online customers. We will 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 New Authentication Strategy**

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

[1] 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.

The following are key components of our authentication strategy:

- **Enrollment and Identity Verification** – We will collect identifying data and use SSA and EDS records to verify an individual's identity. Individuals will 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 will also 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 will self-select a username and password, both of which will be of variable length and alphanumeric. We will provide a password strength indicator to help the individual select a strong password. We will also ask the individual to choose challenge questions for use in restoring a lost or forgotten username or password.

- **Enhancing the User ID** – If individuals opt to enhance or upgrade their User IDs, we will mail a one-time-use upgrade code to their verified residential addresses. 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 will also ask the individual to enter a cell phone number. We will send an initial text message to that number and require the individual to confirm its receipt.

- **Login and Use** – Standard authentication will provide an individual with a User ID for access to most online applications. Enhanced authentication will use 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 will have to log in with their User ID every time they want to access Social Security's secured online services.

We will use this collection of identity proofing and authentication information to verify the identity of the individuals attempting to access our automated services. After we verify individuals' identities, we allow them to create credentials (Usernames and Passwords) they can use to log into and gain access to our secured, automated services. We will also use this information to provide second factor authentication.

SSA will require the individual to agree to the "Terms of Service" detailed on our web site before we allow him or her to begin the enrollment process. The "Terms of Service" inform the individual what we will and will not do with his or her 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 the individual's identity, we will then 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 will send a subset of this information to the EDS, who will then generate a series of out-of-wallet questions back to the individual. The individual will have to answer most of the questions correctly before continuing in the process. The exact questions generated will be 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 or automated 800 number. We will 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 this 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 will only collect the identity verification information one time, when the individual registers for a credential. We will ask for the User ID (Username and password) every time an individual logs in to our automated services. If individuals opt for the enhanced or upgraded account, they will also receive a text message on their cell phones (this serves as the second factor for authentication) each time they log in.

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

We will collect this information electronically via the Internet through SSA's public-facing website: www.socialsecurity.gov, under the agency's Government Paperwork Elimination Act plan. We will 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 will provide the information to a SSA representative during a field office interview. The representative will enter the information via an Intranet customer service application. We expect no more than 25 percent of respondents

will use the in-person process to register for a User ID. We expect no less than 75 percent of respondents will 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 new 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
- RISPA – Request for Internet and Automated 800# Services – Password Authentication for the Individual, OMB #0960-0632
- IRES – Single Sign-On (SSO) & Integrated Registration Services for Business Services Online (BSO), OMB #0960-0626

Further, the new identity verification, public credentialing, and authentication process will absorb and replace these existing collections. We plan to accomplish this work through a series of annual releases. The first release of the new process will not affect the current burden of these existing collections; however, later 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 not being able 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 June 1, 2011 at 76 FR 31671, and SSA received no public comments. The second Notice published on August 1, 2011

at 76 FR 45902. If SSA receives any comments in response to the 30-day Notice, we will forward them to OMB.

We conducted usability testing with members of the public, both beneficiaries and non-beneficiaries. We consulted with special interest groups, including several privacy experts, advocacy group representatives, and other government agencies while we were developing this process. (See the attachment titled, "Discussions with Privacy Experts" which documents the list of stakeholders we consulted and briefed.) We asked these various individuals for their thoughts on our proposed process, since we believe their experience gave them a unique perspective on the issues we were addressing. Based on their feedback, we made policy changes, language changes, and workflow changes to our 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 are asking questions of a sensitive nature in this Information Collection. We will ask the responder some knowledge-based, "out-of-wallet" questions. We may ask the responder for financial information, and we will ask the responder some "shared secret" questions. Before we ask for any information, the responders must read, and agree to our "Terms of Service," which will serve to acknowledge/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 are using them to protect and verify an individual's identity. We must ensure only the true individual can access his or her 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 will not have access to the information the individual provides to the EDS, nor will we retain or have access to any of this information – questions and answers – after the transaction has taken place.

**Financial Information**

We may ask the individual to provide financial account information. If individuals want extra security, we will 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 individual provides will not allow us to access or view his or her 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 will collect shared secrets from the individual to use as password reset questions or username recall functionality in order to improve customer service and reduce workloads and costs. If the individual loses or forgets the password and/or username, we will ask the three questions we established with the individual during account setup when he or she originally created the User ID. The individual must provide correct answers, consistent with the answers on record, to all three questions.

We will ask the individual to select and answer three password reset questions. We have grouped these questions into three sets that deal loosely with persons, places, and things. The individual must select one question from each of the following sets:

**Set 1 – Relationship Questions**

- What is the middle name of your mother?
- What is the middle name of your father?
- What is the first name of your first nephew?
- What is the first name of your first niece?
- What is the name of your first pet?
- What is your maternal grandmother's maiden name?
- What is your paternal grandmother's maiden name?
- What is your oldest sibling's middle name?
- What is your oldest cousin's first name?
- What was the last name of your third grade teacher?

**Set 2 –Geographic Questions**

- What is the name of the hospital where you were born?
- What is the name of the city where your maternal grandfather was born?
- What is the name of the city where your paternal grandfather was born?
- In what city did you meet your spouse/significant other?
- What street did you live on in third grade?
- In what city or town did your mother and father meet?
- Where were you when you first heard about 9/11?
- Where were you when you first heard about JFK being shot?

**Set 3 – Objective Questions**

- What was the model name of your first car?
- What is the color of your first car?
- What is your dream car?
- What was your major or minor in college?
- What was your childhood phone number including area code?
- What was the name of your first stuffed animal?
- What is the first name of your first girlfriend or boyfriend?
- What is the name of your favorite childhood friend?

**12. Estimates of Public Reporting Burden**

We estimate that 17,900,000 requestors will 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 will take an average of 8 minutes to complete a transaction, resulting in an annual reporting burden of 2,386,667 hours. We did calculate a separate cost burden for this process.

We estimate that 5,800,000 requestors will use the In-Person Intranet process annually to create an account with us. We estimate that it will take an average of 8 minutes to complete this transaction, resulting in an annual reporting burden of 773,333 hours. We did not calculate a separate cost burden for this process.

We are using different modalities to collect the information. Since this is a new information collection, we estimated the number of respondents by taking a percentage of the current annual recipients of the Social Security Statement and added a percentage of the current number of beneficiaries who request post-entitlement actions. We estimated the number of minutes for completion by averaging the "time-on-task" figures we obtained from our usability testing.

| **Modality of Completion** | **Number of Respondents** | **Frequency of Response** | **Average Burden Per Response (minutes)** | **Total Annual Burden Hours (hours)** |
|---|---|---|---|---|
| Internet Requestors | 17,900,000 | 1 | 8 | 2,386,667 |
| In-Person (Intranet) Requestors | 5,800,000 | 1 | 8 | 773,333 |
| **Totals:** | **23,700,000** | | | **3,160,000** |

The total annual burden for this information collection is **3,160,000** hours. This figure represents burden hours, and we did calculate a separate cost burden for the respondents using the Internet process. See the next section for details.

**13. Annual Cost to the Respondents**

There is no cost burden to the In-Person Intranet respondents. However, for the Internet responders, there may be some cost if the responder chooses extra security, since this is an optional service. Each time the responder logs in to access SSA's secured online services, we will send a text message to his or her cell phone, which he or she must then enter on the web page.

**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.

**14. Annual Cost to Federal Government**

**EDS Costs**

A key component of SSA's new authentication process, which will manifest 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. We estimate for FY 2011, development and maintenance costs will be $850,000; and transaction costs as $200,000 (based on approximately 500,000 transactions – both Internet and Intranet combined), totaling $1,050,000. For FY 2012, we estimate development and maintenance costs will be $640,000; and transaction costs as $9,480,000, totaling $10,120,000. The amount of the average cost per transaction is approximately 40 cents.

**Social Security Costs**

Social Security's internal cost to build this new process is approximately $6,425,012 for FY 2011. Social Security's internal cost to build this new process is approximately $1,721,621 for FY 2012.

**Total Social Security & EDS Costs**

The total FY 2011 cost to the Federal Government is approximately $7,475,012. The total FY 2012 cost to the Federal Government is approximately $11,841,621. This estimate is a projection of the cost for developing the Internet and Intranet applications, the Client PIN/Password migration, and other supporting processes.

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

This new information collection will create a public reporting burden. See section 12 for estimated burden figures. Eventually, this new identity verification, public credentialing, and authentication process will absorb and replace the existing authentication collections. We plan to accomplish this work through a series of annual releases.

The first release of the new process will not affect the current burdens for the authentication collections listed under OMB Control Numbers 0960-0596, 0960-0632, and 0960-0626; however, later releases will reduce their burden. SSA will prepare change requests for the 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.