This document is scheduled to be published in the
Federal Register on 04/16/2014 and available online at
http://federalregister.gov/a/2014-08578, and on **FDsys.gov**

4191-02-U

SOCIAL SECURITY ADMINISTRATION

Agency Information Collection Activities: Proposed Request

The Social Security Administration (SSA) publishes a list of information collection packages requiring clearance by the Office of Management and Budget (OMB) in compliance with Public Law 104-13, the Paperwork Reduction Act of 1995, effective October 1, 1995. This notice includes revisions of OMB-approved information collections.

SSA is soliciting comments on the accuracy of the agency's burden estimate; the need for the information; its practical utility; ways to enhance its quality, utility, and clarity; and ways to minimize burden on respondents, including the use of automated collection techniques or other forms of information technology. Mail, email, or fax your comments and recommendations on the information collection(s) to the OMB Desk Officer and SSA Reports Clearance Officer at the following addresses or fax numbers.

(OMB)

Office of Management and Budget

Attn: Desk Officer for SSA

Fax: 202-395-6974

Email address: OIRA_Submission@omb.eop.gov

(SSA)

Social Security Administration, OLCA
Attn: Reports Clearance Director
3100 West High Rise
6401 Security Blvd.
Baltimore, MD 21235
Fax: 410-966-2830
Email address: OR.Reports.Clearance@ssa.gov

The information collections below are pending at SSA. SSA will submit them to OMB within 60 days from the date of this notice. To be sure we consider your comments, we must receive them no later than **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Individuals can obtain copies of the collection instruments by writing to the above email address.

1. **Letter to Landlord Requesting Rental Information -- 20 CFR 416.1130(b) -- 0960-0454.** SSA uses Form SSA-L5061 to obtain rental subsidy information, which enables SSA to determine and verify an income value for such subsidies. SSA uses this income value as part of determining eligibility for Supplemental Security Income (SSI) and the correct amount of SSI payable to the claimant. SSA bases an individual's eligibility for SSI payments, in part, on the amount of countable income the individual receives. Income includes in-kind support and maintenance in the form of room or rent, such as a subsidized rental arrangement.

SSA requires claimants to assist in obtaining this information to prevent a delay or overpayment with their SSI payments. We collect this information only if the SSI applicant or recipient is the parent or child of the landlord (respondent). For most respondents, we collect this information once per year or less, via telephone or face-to-face personal interview. The claims representative records the information in our Modernized SSI Claims System (MSSICS), and we require verbal attestation in lieu of a wet signature. However, if the claims representative is unable to contact the respondent via the telephone or face-to face, we print and mail a paper form to the respondent for completion. The respondent completes, signs, and returns the form to the claims representative. Upon receipt, the claims representative documents the information in MSSICS or, for non-MSSICS cases, faxes the form into the appropriate electronic folder and shreds the paper form. The respondents are landlords who are related to the SSI beneficiaries as a parent or child.

Type of Request: Revision of an OMB-approved information collection.

Modality of Completion	**Number of Respondents**	**Frequency of Response**	**Average Burden Per Response (minutes)**	**Estimated Total Annual Burden (hours)**
SSA-L5061	72,000	1	10	12,000

2. **Social Security's Public Credentialing and Authentication Process -- 20 CFR 401.45 and 402 -- 0960-0789.**

Background

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 comprises three distinct factors: something you know, something you have, and something you are. Single-factor authentication uses one of the factors, and multi-factor authentication uses two or more of the factors.

SSA's Public Credentialing and Authentication Process

SSA offers 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 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.

Public Credentialing and Authentication Process Features

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 that we published in the Federal Register (75 F.R. 79065). The PII may include the users' 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 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 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 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 awarded a competitively bid contract to an external data service provider, Experian[1], 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 that balance usability and security. We will 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

[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.

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 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 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" informs 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 the individual's identity, we ask the individual to give us minimal personal information, which may include:

- Name;
- SSN;
- 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 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 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.

The respondents are individuals who choose to use the Internet or Automated Telephone Response System to conduct business with SSA.

Type of Request: Revision of an OMB-approved information collection.

Modality of Completion	**Number of Respondents**	**Frequency of Response**	**Average Burden Per Response (minutes)**	**Total Annual Burden Hours (hours)**
Internet Requestors	38,251,877	1	8	5,100,250
In-Person (Intranet) Requestors	1,370,633	1	8	182,751
Totals	**39,622,510**			**5,283,001**

Date: April 10, 2014.

Faye Lipsky

Reports Clearance Director

Social Security Administration

[FR Doc. 2014-08578 Filed 04/15/2014 at 8:45 am;

Publication Date: 04/16/2014]