

**Addendum to Supporting Statement for
Request for Internet Services – Password Authentication (RISPA)
OMB No. 0960-0632**

SSA is seeking clearance from OMB for a full revision of the Request for Internet Services – Password Authentication (RISPA) and Password Services for the Individual, OMB No. 0960-0632. We are revising the identifying elements used for authentication of identity of requestors of certain services SSA provides over the Internet and via the automated telephone system. In the existing paper processes, individuals who request personal information from SSA records are asked to provide certain identifying information to verify their identity. As an extra measure of protection, SSA asks requestors who use its Internet services to provide additional identifying information so that SSA can authenticate their identity before releasing or updating personal information. The additional identifying elements are unique to the Internet and not asked for in comparable paper forms. Clearing the Internet identification elements separately allows the Agency to place electronic versions of comparable paper forms on the Internet without having to clear these versions through OMB because they ask for more identifying information than the paper form.

Time It Takes Statement

We estimate that the completion of the identifying elements takes 1 - 2 minutes (average time, 1½ minutes) and the completion of the actual Password Services pages (which includes the 2 to 3 minutes it takes to complete the surveys) takes 8 – 9 minutes (average 8½ minutes), with an average of about 2 ½ minutes for the completion of each step in the process. The total estimate for completion of the process averages at about 10 minutes. The requester completes both the identifying information and the information specific to the request (e.g., a request for a Password Request Code; a request to register a Password; a request to change a Password; and a request to use the Password, along with a User ID – SSN - to authenticate and gain access to other protected SSA services) and then submits the request through the Internet or via the automated telephone services. It is not apparent to the beneficiary that there are separate burdens for the identity questions and the application questions. Therefore, the estimate shown on the actual screens for the specific activity is a total of the estimate for the two information collections. Providing the “time it takes” estimate in a single statement imposes less burden on the public because they will need to read only one statement.

Number of Respondents and Annual Burden

The number of respondents and annual burden for the various online Internet and automated telephone services, apart from the Password Services, are cleared under separate OMB numbers. It was simpler to include the burden for the specific application questions under the respective OMB clearance packages. Therefore, we did not include the additional burden for these services in this clearance request. However, this clearance request does include the burden on the public for the Internet and automated telephone Individual Password Services.

Flow of Pages in the Authentication Process

The process for authentication will begin after the individual indicates that he or she wants:

- to Get a Password Request Code (PRC);
- to Register a Password;
- to Change a Password; or
- to use a password to gain access to other electronic/automated services.

The authentication process works as follows. To get a PRC or register a password, the first page requires the individual to provide personal identifying information - Social Security Number (SSN), Date of Birth, and Name. (In the case of registering a password, the user must also supply his or her assigned PRC in order to activate the password process.) To change a password or to use a password to gain access to protected applications, the first page requires the individual to provide the password in conjunction with a User ID (SSN). Upon successful authentication, the user proceeds to the specific application pages.

Questions Asked

Beginning in 2001, SSA set up Password Services for individuals using the Internet and the automated telephone services. Information provided by the individual was matched with SSA's NUMIDENT file and Master Beneficiary Record (MBR). SSA required the individual to provide certain subsets of the following information, depending on the transaction.

- Social Security Number (SSN)
- Date of Birth (DOB)
- Password Request Code
- Confirmation Number
- Last Payment Amount
- Last 4 digits of direct deposit account number
- Current Password

Our review of this process has shown that there is a high exception rate for Confirmation Number, Last Payment Amount, and Last 4 Digits of the Direct Deposit Account Number. While we do not want to promote persons who are trying fraudulently or otherwise to access information that does not belong to them, we do want to reduce the exception rate for persons to whom the records belong and who want to use these services. Consequently, we have decided to drop these 3 troublesome pieces of information when we convert our Password Services to the Access Control Utility (ACU).

Changes in Collection Information Made to Existing Password Services

On September 23, 2006, we are converting our Password Services to the ACU. Due to the conversion of our Individual Password Services to the ACU, we are adding some information to Password Authentication (PWA) and dropping some information from PWA. We must do this in order to successfully convert these services so that they fit into the approved ACU Authentication schema. The necessary changes to PWA are: add Name as an authentication data element and remove Confirmation Number, Payment Amount, and last 4 digits of the Direct Deposit Account Number. We will continue to request SSN, Date of Birth, and Password Request Code (PRC - a shared secret created by SSA and mailed or electronically sent to the requestor).

The information collected by Password Services is used to authenticate an individual prior to giving him or her access. SSA will continue to collect and use the information to establish a Password Data File. The file will continue to be used to allow customers to conduct electronic business with the Agency. Eventually, this Password Data file will become part of the LDAP Data File housed within the ACU.

The User ID/Password process will continue to be used for access to SSA's online and automated telephone services. These services will be password-protected when SSA has determined either the information transmitted or the requestor requires a higher level of protection. The User ID/Password may also be used to access electronic services that require a lower level of protection. Some of the services that require password protection include, but are not limited to:

- Change of Address and Telephone Number;
- Direct Deposit Elections or Changes; and
- Account Status Inquiries.

The Password process will continue to allow the requestor to establish his or her identity with SSA, create a Password, and use that password, along with a User ID (Social Security Number), to access or change his or her own personal information maintained by SSA. We will also continue to allow customers to change their password, and for those who have lost or forgotten their Password, to re-establish their identity with us and create a new Password.

Prior to getting a Password Request Code (PRC), we will verify the requestor's identity. We will ask for the following information:

- SSN;
- Date of Birth; and
- Name.

If the requestor passes authentication, we will mail the PRC in a letter to the address we have on our records.

Prior to creating a Password, we will verify the requestor's identity. We will ask for the following information:

- Shared secret created by SSA and mailed to the requestor (the Password Request Code or PRC used for activation);
- SSN;
- Date of Birth; and
- Name.

Prior to changing a password and granting access to authorized applications, we will authenticate the requestor using the following information:

- User ID (SSN)
- Current Password

Answers to these questions are then compared to information contained in our records.

Other Changes

Another change we are making effective September, 2006, will affect the Block Electronic Access process. We are taking the password out of the block access process. This means that the user will no longer have to enter his or her password as an authentication element when he or she is trying to block all electronic/automated access to his or her personal information. Previously, we verified the user with SSN and Password or with SSN and Date of Birth. Effective September, 2006, we will authenticate using only SSN and Date of Birth.

We are introducing 2 surveys to the Password Services process. These will help us to collect information about the process, itself. The surveys will help us to identify problems in the process and they will reinforce what works well for users. Survey responses will help us to improve our password process. The 2 surveys are:

- the Password Services Survey; and
- the Password Services Exit Survey.

These surveys will capture information from users who complete the process successfully and from users who exit the process early without completing the task.

Automated Telephone Applications

We will be making the same changes to the automated telephone Password Services within the same timeframe.

Collection Instruments

Attached are four documents. Two are the collection instruments, the Internet application screens and the automated telephone services screens. Also attached are examples of two letters sent to respondents that gives the password request code or gives instructions on changing their password. These letters provide the information the respondent must give in order to choose a password and access their records.