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

Release 1 of the New Process

For the first release of this new authentication process, we are targeting individual services for online access. The respondents we are targeting are current Social Security beneficiaries and recipients, as well as the general public. After individuals register for a credential and pass authentication, they may have access (if they pass authorization), via a Landing Page, to the following applications:

- Online Statement
- Internet Benefit Verification
- Internet Change of Address
- Internet Direct Deposit
- Internet Check Your Benefits
- Security Settings

For the first release of this new process, we will register individuals via the Internet or via the in-person process in the field. Individuals will only be able to use their UserID to access the Social Security Administration's (SSA) online protected services on behalf of themselves. We are not allowing access to the existing automated telephone PIN/Password versions of these applications using the new credential with this release.

We decided the actual applications individuals are accessing using this new authentication process would **not** fall under this authentication clearance package. Any Internet or Automated Telephone service that requires authentication must have its own separate OMB clearance, if one is required.

We do not intend to continue the practice of mixing electronic applications with identity proofing and authentication methods in the same clearance package. The scope of this package covers all activities associated with establishing an account with SSA, registering a credential, managing that account, and authenticating with the credential. It does **not** cover the various other online services the individual can access using that credential after he or she has successfully passed authentication.

The agency is currently developing a strategy for a controlled rollout of the new process and the applications that go behind it. We plan to implement the first release effective with the end of January 2012. Our new public credentialing and authentication process will first give access to the online Social Security Statement for non-Social Security beneficiaries and to the online applications (mentioned above) for our Social Security beneficiaries. With this release, we will also be implementing the "grandfathering" process.

Grandfathering Current Client PIN/Password (Internet PPW) Users

"Grandfathering" is the business process that describes how individuals who currently conduct business online with SSA, using an existing client PIN and password (PPW), may obtain a credential through the new process. Conversion of the PPW credential involves issuing a new User ID at assurance level 2 predicated on possession of an existing level-2 credential with us.

Individuals may elect to log into an online SSA service (that is behind the new process) with a client PPW credential. Individuals are then required to obtain a new credential through an abbreviated version of the new process. Holders of these legacy credentials will be able to bypass the identity-proofing components of the new process and immediately obtain a new User ID by entering the Account Setup process and providing an e-mail address, a password, and password reset questions and responses. (Note that we will not be calling the EDS as part of the grandfathering process.) Upon successful validation, we create a new account for the individual and redirect him or her to the requested SSA service using the newly established credential.

SSA considers the issuance and management processes for PPW credentials to satisfy NIST guidance for a level-2 credential. Allocation of the new credential for the existing user is a re-issuance process of an existing credential rather than a new enrollment/issuance process. While NIST SP 800-63 does not specify a separate re-issuance process, NIST 800-63 rev. 1 (draft) indicates that re-issuance is allowable at level 2 if the applicant provides proof of possession of the current unexpired token at assurance level 2. The Kantara Initiative Service Assessment Criteria §3.7.3.2 additionally reflect the NIST 800-63 rev.1 specifications for credential re-issuance.

Because providing a new credential to grandfathered users is a re-issuance process, there is no policy obligation to conduct identity proofing again; we would have performed compliant identity proofing when originally issuing the PPW credential. Consequently, we will neither re-verify the confirmed address of record with external sources nor conduct an out-of-wallet quiz.

The PPW credential remains valid after we grandfather it, and the users can continue normal use for legacy applications that require a PPW credential. Users cannot use PPW credentials to access the new authentication process-enabled applications, except through this grandfathering process.

Once all PPW-enabled applications are using the new authentication process, we may not issue new password request codes (PRC) for new Internet PPW credentials through any other mechanism. Users may continue to use unexpired PRCs to create new PPW credentials. Since the user needs a PRC to establish a new Internet PPW credential, it follows that SSA will issue no new Internet PPW credentials once all new Internet PRCs have expired.

In-Person Process and Customer Support

We are offering an alternative in-person identity proofing and 800 Number telephone customer support process for those who are uncomfortable with, or unable to use, the Internet process. This Customer Support application is an intranet application that provides an interface for authorized personnel to respond to customers' requests for service.

The SSA 800 Number staff will have the ability to complete the following operations after verifying the user's identity through standard processes:

- Remove remote lockouts and reset all counters/strikes to zero on the User ID;
- Deactivate a User ID;
- De-elevate a User ID from enhanced (Level 3) to standard (Level 2);
- Change attributes attached to the User ID, excluding password reset questions, provided we have authenticated the user at a level of assurance equal to or exceeding the maximum level of assurance assigned to the User ID;
- View the username associated with a User ID;
- Provide general assistance with the public user interface through internet screen facsimiles and notice facsimiles;
- Search for User IDs by Social Security Number (SSN) and username;
- Send a temporary password for a Level-2 User ID to the email address of record in event of unknown password reset questions; and,
- Cancel a temporary password request.

SSA field office staff can complete all functions available to 800 Number staff after verifying the user's identity through standard in-person processes. Additionally, SSA field office staff can:

- Conduct in-person identity proofing for credential issuance/enrollment;
- Provide an elevation code for an enhanced User ID. SSA staff will have the ability to reprint any enrollment or elevation code generated via RCS provided they have not left the print screen. If the staff person has left the screen or closed the record, they will have to re-input the process and generate a new code;
- Reset a password to a temporary password and issue an email containing the temporary password to the user. The user will be required to change the password online at first login; and,

- Provide an optional printed receipt of certain actions taken in RCS at the request of the customer.

Information About the External Data Service

Who is Experian?

Experian is a global information services company. Experian's decisional solutions enable SSA to manage and optimize risk, as well as prevent, detect and reduce fraud.

What does Experian do for SSA?

SSA will collaborate with Experian, an external authentication service provider, to help us verify the identity of our online customers and to prevent fraudulent access to individuals' sensitive information. Specifically, Experian's tools help verify an individual's identity and prevent identity fraud by:

- Providing and grading knowledge-based authentication (out-of-wallet) questions designed to be readily answered by true identity owners, but not identity thieves;
- verifying addresses; and,
- verifying financial account information.

SSA will collect the personal information and verify it against our own databases and against Experian's databases. We keep the data sources separate, and we are not sharing SSNs with Experian. Experian will not keep any information we share with them except as required by Federal laws, regulations, or guidelines.

SSA will not save out-of-wallet transaction data from Experian, nor are we basing any decisions regarding Social Security benefits on Experian data. This partnership enables identity verification while protecting identity data.

Experian's Out-of-Wallet Questions

Experian provides a knowledge-based authentication solution. It 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. Experian designs the questions they ask so that only the individual would know the answer. If someone stole his or her wallet, that identity thief should not be able to answer these questions.

Here are some sample questions similar to those Experian uses for the out-of-wallet quiz. These sample questions are sufficiently representative of the entire set of questions Experian may ask.

- In which of the following cities have you previously lived?
- Which of the following is a previous phone number?
- You took out a student loan in 1999. Who was the lender?

ATTACHMENTS

A. Internet Screens

The complete notice library is available upon request.

B. RCS Intranet Screens

Customer service notices are included in the Intranet screens package.

C. SORN

D. Privacy Act Statements

E. Paperwork Reduction Act Statement

F. Authoring Laws and Regulations List

G. Discussions with Privacy Experts List

H. Social Security’s Authentication Process