

**Addendum to Supporting Statement for
Request for Internet Services – Password Authentication (RISPA)
20 CFR 401.45
OMB No. 0960-0632**

Terms of Clearance

OMB is approving this collection for 36 months with the condition that SSA will conduct a new risk assessment each year, as required by OMB memorandum M-04-04, to determine the appropriateness of the authentication and verification standards employed. A written summary of the results of the risk assessments should be shared with OMB as part of any future requests for approval. In performing these risk assessments, SSA should comply with all OMB guidance and National Institute of Standards and Technology standards. The agency should also consult any guidance from the Chief Information Officers Council.

SSA has not met these Terms of Clearance, as we are eliminating Request for Internet Services – Password (0960-0632) due to low volume usage.

Instead, we will be “grandfathering” current Pin Password users to the new Public Credentialing and Authentication Process covered under OMB # 0960-0789. In addition, we will be transitioning all current Pin Password automated telephone users to the new Citizen Access Routing Enterprise (CARE) system. Since the CARE system will no longer require Pin Password services, we will cover CARE under our Knowledge Based Authentication process (0960-0596). We expect to discontinue the current Pin-Password process (0960-0632) by the end of calendar year 2012, therefore, we did not see any reason to conduct another risk assessment.

As mentioned in the Addendum for our new Public Credentialing and Authentication Process (0960-0789), our first release gives access to the online Social Security Statement for non-Social Security beneficiaries. Our second release, scheduled for the end of the calendar year, 2012, gives access to the following online applications for our Social Security beneficiaries.

- Internet Benefit Verification
- Internet Change of Address
- Internet Direct Deposit
- Internet Check Your Benefits

With our second release, we will begin implementing the “grandfathering” process for the current Pin Password Services (0960-0632). Through this grandfathering process, we will allow individuals who currently conduct business online with SSA using the existing Pin Password to obtain credentials through the new process.

SSA worked with privacy experts and NIST to create the new Public Credentialing and Authentication Process. In doing so, we conducted several risk assessments, as mandated

by OMB memorandum M-04-04. We discussed this in detail within the Information Collection Request OMB approved for 0960-0789 on 9/30/11. In addition, we expect to continue to conduct the mandated risk assessments for the new Public Credentialing and Authentication Process (0960-0789). However, as mentioned above, we will not conduct risk assessments for 0960-0632 as we intend to discontinue it by the end of this fiscal year.

Revisions to the Collection Instrument

Removal of Password Authentication for Automated Telephone Applications

The agency made a decision to eliminate the current Password Authentication (Pin and Password) option for the automated telephone applications due to low volume of usage by the following automated telephone applications:

- Password Services
- Change of Address (COA)
- Direct Deposit (DD)
- Check Your Benefits (CYB)

Moreover, the expected volume of usage did not justify the expenses associated with transitioning the automated telephone applications associated with Pin and Password to the new Citizen Access Routing Enterprise (CARE) through 2020. When we transition to CARE, we will remove the CYB and Password Services applications service, since it is Pin/Password only. We do not plan to replace these automated telephone applications; however, we will continue to use the Knowledge Based Authentication (KBA 0960-0596) for COA and DD after the transition. Individuals who wish to do business with us electronically, will need to use the Internet for CYB and Password Services.

The final factor was the agency's decision to move forward with implementing a more stringent authentication protocol called the Public Credentialing and Authentication Process. The new authentication process received approval from the Office of Management and Budget (OMB) under OMB clearance number 0960-0789.

The new authentication process would require the use of a user identification (ID) and an 8-digit, alphanumeric, case-sensitive password. The format of the user ID and password is not conducive to telephone use. Therefore, the automated telephone applications mentioned above cannot accommodate the use of the new user ID and password for authenticating callers.

We anticipate that the Pin and Password discontinuance will become effective in FY2012 after we transition the National 800 Number Network (N8NN) to CARE.