Supporting Statement for
Social Security Administration's Public Credentialing and Authentication Process
20 CFR 401.45, 20 CFR 402
OMB No. 0960-0789

A. Justification

1. Introduction/Authoring Laws and Regulations

The Social Security Administration (SSA: we, us, etc.) is continuing its public credentialing and authentication process that provides secure access to SSA's electronic services.

SSA collects and maintains the customers' personally identifiable information (PII) in our *Central Repository of Electronic Authentication Data Master File* Privacy Act system of records, which we published in the Federal Register (December 17, 2010, at 75 FR 79065). The PII may include but is not limited to the customer's full name, address, date of birth, Social Security number, 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 USC 6103(l)(1)A)*]. SSA may also collect knowledge-based authentication data, which is information customers establish with us or that we already maintain in our existing Privacy Act system of records.

SSA retains the data necessary to administer and maintain our Digital Identity 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.

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, as amended), Internal Revenue Code (*26 U.S.C. § 6103(l)(1)(A)*), Federal Information Security Modernization Act of 2014 (*Title III*) of the E-Government Act of 2002 (*Pub.L. 107-347,* section *301*), and OMB Circular No. A-130.

2. Description of Collection

The SSA offers a number of services through its *my* Social Security web application. Because these services include sensitive and personal information about earnings records, as well as the opportunity to submit and track certain benefits applications, it is critical that Social Security ensures an individual's identity is properly verified and credentialed prior to granting access to *my* Social Security. This information collection establishes the information we must solicit to authenticate identities both remotely and in-person. SSA continually develops new methods for credentialing identities both remotely and in-person to facilitate ease of use while also upholding stringent identity verification requirements.

SSA partnered with the General Services Administration's Login.gov in May 2021, but still maintains our own credentialing as an option for users. Therefore, customers were able to create an account with Login.gov, or elect to create one with us. To provide additional security, if customers have an existing Login.gov account with Identity Assurance Level (IAL)1 (no identity verification via Login.gov) we require them to identity proof to an IAL2 account during their first sign in attempt. This Federated Identity System (FIS) partner uses the same federal guidelines and principles used by SSA when registering customers. If customers are able to reuse existing credentials, it saves them time and effort because they do not have to go through the *my* Social Security registration process. Furthermore, they do not have to maintain another set of credentials.

In September 2021, we made additional changes that were OMB approved. When customers access SSA's website to sign into their accounts, SSA's website now presents the customers with a choice to sign in with an eAccess credential or to sign in with a Login.gov or ID.me credential. SSA no longer allows customers to create credentials directly through eAccess. For all new accounts, customers must choose to create a credential with ID.me or Login.gov.

Additionally, a subsequent release in March 2023, focused on the beginning of the migration of applications from our Integrated Registration Services (IRES) System (OMB No. 0960-0626) to our eAccess platform. This OMB approved release allowed SSA to require IRES users who need access to the Employer Wage Reporting (EWR) and Social Security Number Verification Service (SSNVS) applications to authenticate through eAccess rather than IRES to enhance the security for these business services.

Our public credentialing and authentication process:

- Issues a single User ID through Login.gov or ID.me to any enumerated customer who wants to do business online with the agency and meets the eligibility criteria;
- Partners with an external Identity Services Provider (ISP) to provide data for us to verify the identity of our online customers;
- Offers access to some of some SSA's most pertinent, but more sensitive, workloads online while providing us an acceptable level of confidence in the identity of the person requesting access to these services;
- Offers an in-person identity verification process for those who are uncomfortable with, or unable to use, the online process;
- Uses a risk-based approach to balance security, ease of use, compliance, cost, and feasibility consideration; and
- Provides a user-friendly means for the public to conduct extended business with us online instead of visiting local servicing offices or requesting information over the phone.

SSA uses the information from this collection to identity proof and authenticate our customers online and to allow them access to their personal information from our records. SSA also uses 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 our goals, but is vital to good public service. In increasing numbers, the public expects to conduct complex business online. Ensuring our online services are both secure and user-friendly is our priority. With the limited data we have, it is difficult for us to meet the OMB and National Institute of Standards and Technology (NIST) authentication guidelines for identity proofing the public. Therefore, we awarded a competitively bid contract to an ISP, Experian[1], to help us verify the identity of our online customers. We use this ISP, 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 Digital Identity Strategy

We remain committed to enhancing our online services using digital identity processes, which balance usability and security. We continue to research and develop new digital identity capabilities while monitoring emerging threats. All customers must access our www.ssa.gov/myaccount website to choose to create an account or sign in. There are also links on the main homepage www.ssa.gov that allow users to sign in or obtain information about the registration process and to what the accounts allow access.

The following are key components of our digital identity procedures:

Enrollment and Identity Verification

Individuals who meet the following eligibility requirements may enroll:

- Must have a valid email address;
- Must have a valid Social Security number (SSN);
- Must have a domestic address of record (includes military addresses); and
- Must be at least 18 years of age.

We may ask the customer to provide certain financial information (e.g., Medicare wages, self-employed earnings, the last eight digits of a credit card number or the last direct deposit amount from Social Security benefits) for verification. We may also ask individuals to answer out-of-wallet questions so we can further verify their identities or input driver's license or state identification information. Individuals who are unable to complete the process online can present identification at a field office to obtain a User ID.

- **Establishing the Credential** – This process is now handled through either the Login.gov or ID.me credentialing process.

- **Provide an Enrollment Code**

[1] Experian is a global information solutions provider. Experian's solutions help Social Security to manage risk and mitigate fraud.

When the customer adds a state ID, we provide a one-time enrollment code to a verified address that the customer provided during this process. To create an advanced credential, the customer must enter the enrollment code received. The address of record could be digital (email or SMS text to a cell phone), or it could be the customer's physical address. If the customer receives the enrollment code digitally and it is successfully verified, this digital address is automatically set up as the customer's second factor of authentication. Customers who receive an enrollment code via mail may return at a later time to enter their second factor and finish setting up the account.

- **Sign in and Use** – Login.gov and ID.me provides the authentication process for our customers to have access to our sensitive online Social Security services.

Remote Identity Proofing Process

The in-person enrollment process is a one-time only activity offered to individuals who cannot, or are not willing to register for an account via the Internet. For the in-person process, the individual must go to a local SSA field office and provide identifying information. SSA requires individuals to agree to the "Terms of Service" and "Privacy Act" statements that are handed to them or read aloud to begin the enrollment process. The "Terms of Service" and "Privacy Act" inform the individuals what we will and will not do with their personal information and provides the privacy and security protections on all data we collect. These terms also detail the consequences of misusing this service.

To verify an individual's identity, we ask the individual to give us personal information, which may include:

- Name;
- Social Security number;
- Date of birth;
- Residential mailing address;
- Phone number (suggested);
- E-mail address (recommended); and
- State Identification Documents (Driver's License, Learner's Permit, or State Identification Card information).

SSA sends a subset of this collected information to the ISP for verification. SSA only collects the identity verification information one time when the individual registers for a credential. Once verified, SSA will provide the customer with an activation code for their online account.

Psychological Costs

We have not identified any psychological costs based on the requirements for this information collection. Since there are no psychological costs, we have not included this potential psychological cost into account when calculating our burden in #12 below.

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

3. Use of Information Technology to Collect the Information

SSA collects this information electronically via the Internet through our public-facing website, www.socialsecurity.gov, under the agency's Government Paperwork Elimination Act plan. We 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 provides the information to an SSA representative during a field office interview. The representative enters the information via an Intranet customer service application. Approximately 2 percent of respondents use the in-person process to register for an account. Approximately 98 percent of respondents use the online process. Approximately 16 percent of the individuals who try to identity proof online are unsuccessful.

4. Why We Cannot Use Duplicate Information

The nature of the information we collect and the manner in which we collect it would normally preclude duplication. Although we currently use other collection instruments to obtain similar data, this 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. Our other authentication processes, listed below, do not include these features.

- RISA – Request for Internet and Automated 800# Services – Knowledge-Based Authentication for the Individual, OMB #0960-0596
- IRES – Single Sign-On (SSO) & Integrated Registration Services for Business Services Online (BSO), OMB #0960-0626

Further, this identity verification, public credentialing, and authentication process will eventually absorb and replace the existing collections (mentioned above). SSA plans to accomplish this work through a series of annual releases. Additional 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 (*NIST SP 800-63*) and the Executive Order 13681. In addition, failure in our ability to verify the requesters' identity would result in our inability 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 September 8, 2023, at 88 FR 62136, and we received no public comments. The 30-day FRN published on November 15, 2023 at 88 FR 78443. If we receive any comments in response to this Notice, we will forward them to OMB.

We will continue to conduct usability testing with members of the public, both beneficiaries and non-beneficiaries, as we build upon and enhance this process. SSA conducts the usability testing under our usability testing customer satisfaction survey, OMB No. 0960-0788.

9. Payment or Gifts to Respondents

Social Security does not provide payments or gifts to the respondents.

10. Assurances of Confidentiality

SSA 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 collect, maintain, and distribute 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 Modernization Act of 2014 (Title III)* of the E-Government Act of 2002 (*P.L. 107-347*), and OMB Circular No. A-130.

11. Justification for Sensitive Questions

SSA asks questions of a sensitive nature in this Information Collection. SSA may ask the respondents some knowledge-based, "out-of-wallet" questions, and we ask the respondents some "shared secret" questions. We may ask the respondents for financial information. Before we ask for any information, the respondents must read, and agree to our "Terms of Service," which serves to acknowledge and 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 our legal authority for collecting the information.

<u>Out-of-Wallet Questions</u>

The ISP incorporates both public and private data to allow generation and evaluation of questions uniquely pertaining to a given consumer. SSA calls these "out-of-wallet" questions. The ISP 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 SSA uses them to protect and verify an individual's identity. SSA must ensure only the true individuals can access their personal information. SSA asks these questions only once, and in multiple-choice format, when the respondent enrolls to create an account with us. (See the screen package for examples of these questions.)

SSA does not have access to the information the individual provides to the ISP. SSA does not retain or have access to any of the information – questions and answers – after the transaction takes place.

Financial Information

SSA may ask the individual to provide financial account information. SSA asks individuals to provide financial account information in the form of W-2 information; self-employment information from tax returns; monthly benefit direct deposit amount; or the last eight digits of a credit card. SSA confirms financial account information as another way of ensuring an individual's identity, using our own records or, in the case of the last eight digits of a credit card, using the ISP's records. The information the individuals provide does not allow us to access or view their financial accounts or credit records. Providing this information is optional. SSA only asks for financial information one time, when the respondent enrolls to upgrade a Social Security account. If the individuals are uncomfortable about giving SSA financial account information, they can still sign up for an account by visiting their local Social Security field office in person. SSA does not require financial information as part of the in-person process.

12. Estimates of Public Reporting Burden

Modality of Completion	Number of Respondents	Frequency of Response	Average Burden Per Response (minutes)	Estimated Total Annual Burden (hours)	Average Theoretical Hourly Cost Amount (dollars)*	Average Wait Time in Field Office (minutes)**	Total Annual Opportunity Cost (dollars)***
Internet Registrations	11,788,914	1	8	1,571,855	$29.76*		$46,778,405***
Internet Sign-Ins	124,989,089	1	1	2,083,151	$29.76*		$6,194,574***

Intranet Registration (RCS)	54,908	1	8	7,321	$29.76*	24**	$871,492***
Totals	**136,832,911**			**3,662,327**			**$53,844,471****

* We based this figure on average U.S. citizen's hourly salary, as reported by Bureau of Labor Statistics data (https://www.bls.gov/oes/current/oes_nat.htm#00-0000).

** We based these figures on the average FY 2023 wait times for field offices (24 minutes) and teleservice call centers (19 minutes), based on SSA's current management information data.

*** This figure does not represent actual costs that SSA is imposing on recipients of Social Security payments to complete this application; rather, these are theoretical opportunity costs for the additional time respondents will spend to complete the application. **There is no actual charge to respondents to complete the application**.

In addition, OMB's Office of Information and Regulatory Affairs is requiring SSA to use a rough estimate of a 30-minute, one-way, drive time in our calculations of the time burden for this collection. OIRA based their estimation on a spatial analysis of SSA's current field office locations and the location of the average population centers based on census tract information, which likely represents a 13.97-mile driving distance for one-way travel. We depict this on the chart below:

Total Number of Respondents Who Visit a Field Office	**Frequency of Response**	**Average One-Way Travel Time to a Field Office (minutes)**	**Estimated Total Travel Time to a Field Office (hours)**	**Total Annual Opportunity Cost for Travel Time (dollars)****
54,908	1	30	27,454	$817,031****

****We based this dollar amount on the Average Theoretical Hourly Cost Amount in dollars shown on the burden chart above.

Per OIRA, we include this travel time burden estimate under the 5 CFR 1320.8(a)(4), which requires us to provide "time, effort, or financial resources expended by persons [for]…transmitting, or otherwise disclosing the information," as well as 5 CFR 1320.8(b)(3)(iii) which requires us to estimate "the average burden collection…to the extent practicable." SSA notes that we do not obtain or maintain any data on travel times to a field office, nor do we have any data which shows that the average respondent drives to a field office, rather than using any other mode of transport. SSA also acknowledges that respondents' mode of travel and, therefore, travel times vary widely dependent on region, mode of travel, and actual proximity to a field office.

NOTE: We included the total opportunity cost estimate from this chart in our calculations when showing the total time and opportunity cost estimates in the paragraph below.

We calculated the following Learning Cost time burden based on the estimated time and effort we expect respondents will take to learn about this program, its applicability to their circumstances, and to cover any additional research we believe respondents may need to take to understand how to comply with the program requirements (beyond reading the instructions on the collection instrument):

Total Number of Respondents	**Frequency of Response**	**Estimate Learning Cost (minutes)**	**Estimated Total Annual Burden (hours)**	**Total Annual Learning Cost (dollars)****
11,788,914	1	15	2,947,229	$87,709,535*****

*****We based this dollar amount on the Average Theoretical Hourly Cost Amount in dollars shown on the burden chart above.

NOTE: We included the total opportunity cost estimate from this chart in our calculations when showing the total time and opportunity cost estimates in the paragraph below.

We base our burden estimates on current management information data, which includes data from actual interviews, as well as from years of conducting this information collection. Per our management information data, we believe that **1 and 8** minutes accurately shows the average burden per response for learning about the program; receiving notices as needed; reading and understanding instructions; gathering the data and documents needed; answering the questions and completing the information collection instrument; scheduling any necessary appointment or required phone call; consulting with any third parties (as needed); and waiting to speak with SSA employees (as needed). Based on our current management information data, the current burden information we provided is accurate. The total burden for this ICR is **3,662,327** burden hours (reflecting SSA management information data), which results in an associated theoretical (not actual) opportunity cost financial burden of **$142,371,037.** SSA does not charge respondents to complete our applications.

13. Annual Cost to the Respondents

There may be a cost burden to the respondents if respondents choose cell phone as the second factor. These costs could be incurred at registration, sign in, or when they contact us over the phone. However, since these costs are associated with the respondent's chosen cell phone carrier, we do not estimate these costs in this ICR to avoid conjecture. Based on our knowledge of current cell phone plans, we estimate the costs could be as follows:

Short Message Service (SMS) cost – code sent via text message using SMS to the individual customer.

- For the customer 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 customer 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 customer who has an unlimited text plan, there would be no charge. The customer would have paid for this service as part of the plan. We have no way to estimate cost. We estimate that 88% of U.S. cell phones have unlimited texting.

14. Annual Cost to Federal Government

The total cost to the Federal Government is approximately **$29,227,142**.

Description of Cost Factor	**Methodology for Estimating Cost**	**Cost in Dollars***
Designing and Printing the Form	Design Cost + Printing Cost	$0
Distributing, Shipping, and Material Costs for the Form	Distribution + Shipping + Material Cost	$0
SSA Employee (e.g., field office, 800 number, DDS staff) Information Collection and Processing Time	GS-9 employee x # of responses x processing time	$820,845
Full-Time Equivalent Costs	Out of pocket costs + Other expenses for providing this service	$0
Systems Development, Updating, and Maintenance	GS-9 employee x man hours for development, updating, maintenance	$28,406,297
Quantifiable IT Costs	Any additional IT costs	$0
Other	[Component may add as needed]	$0
Total		**$29,227,142**

* We have inserted a $0 amount for cost factors that do not apply to this collection.

15. Program Changes or Adjustments to the Information Collection Request

When we last cleared this IC in 2020, the burden was **2,256,275** hours. However, we are currently reporting a burden of **3,684,290** hours. This increase in burden hours stems from the continuing expansion of our online services and the increase in the number of individuals who register for a credential so they can come online to do business with us. In addition, we are removing the individualized burden for Advance Designation users, and are to the Internet Registration users.

Eventually, this identity verification, public credentialing, and authentication process will absorb and replace the existing authentication collections under OMB Control Numbers 0960-0596 and 0960-0626. We plan to accomplish this work through a series of annual releases. The future releases will reduce the burdens in the other existing authentication collections. SSA will continue to prepare change requests for the other existing authentication collections, as needed.

*** Note:** The total burden reflected in ROCIS is **3,684,290**, while the burden cited in #12 of the Supporting Statement is **3,662,327**. This discrepancy is because the ROCIS burden reflects the following components: field office waiting time + a rough estimate of a 30-minute, one-way, drive burden. In contrast, the chart in #12 of the Supporting Statement reflects actual burden.

16. Plans for Publication Information Collection Results

We will not publish the results of the information collection.

17. Displaying the OMB Approval Expiration Date

We are not requesting an exception to the requirement to display the OMB approval expiration date.

18. Exceptions to Certification Statement

We are not requesting an exception to the certification requirements at *5 CFR 1320.9* and related provisions at *5 CFR 1320.8(b)(3)*.

B. <u>Collections of Information Employing Statistical Methods</u>

Social Security does not use statistical methods for this information collection.