**Supporting Statement for Emergency Paperwork Reduction Act Approval For:**
***my* Social Security – Security Authentication PIN (SAP)**
**20 CFR 401.45**
**OMB No. 0960-NEW**
**Emergency Information Collection Request (ICR)**

## A. Justification

### 1. Introduction/Authorizing Laws and Regulations

***Introduction/Overview***

To mitigate fraud concerns, in April 2025, SSA will increase the level of identity proofing needed for respondents to make payment method changes during phone interactions. While necessary to protect the public and the integrity of SSA's programs, these changes will prevent the use of knowledge-based questions to authenticate a respondent's identity prior to making a direct deposit change. To bridge this gap, SSA developed a hybrid identity proofing process called the 'Security Authentication PIN' (SAP) that will provide identity-proofing parity with our online modality, as well as with in-person identity verification for direct deposit requests. Utilizing the SAP process will provide the necessary identity verification to allow direct deposit changes via phone or in person, while ensuring fraud protection through verification of the identity of the individual prior to accessing or revising their account.

Under Sections *20 CFR 401.45* of the *Code of Federal Regulations*, SSA will request individuals who would like to conduct business with SSA for direct deposit changes over the phone, to provide a SAP which utilizes the respondent's *my* Social Security account to generate a one-time passcode. An SSA field office or National 800 Number technician will direct the respondent to access the ssa.gov/pin link using their online Social Security login credentials to generate the one-time use SAP. The respondent will provide the SAP to the technician who will enter it into the Technician Experience Dashboard (TED) to verify the one-time-passcode. If the code validates and the respondent successfully verifies his or her identity, the technician will proceed with resolving the direct deposit request, updating bank information, or effectuating other pertinent payment method requests.

### 2. Description of Collection

***Background***

Our current telephone process requires respondents to use knowledge-based questions to verify their identity that matches SSA's records. Depending upon the situation, the requested information or action, and the judgement of potential misrepresentation of the caller, the SSA technician may ask additional approved questions to verify the respondent's identity. While this process is sufficient fraud protection and authentication under NIST Special Publication 800-63, *Digital Identity Guidelines*, it still poses a fraud risk for respondents who wish to complete tasks for which our automated telephone system, or Internet platforms

would request higher levels of identity proofing and authentication. Knowledge-based methods are susceptible to compromise by fraudulent actors who have become increasingly capable of obtaining the answers to knowledge-based questions. Direct deposit changes provide an opportunity for attackers to convert beneficiary payments to their own use. Consequently, we consider the establishment of or revisions to direct deposit account information to be a higher risk task meriting a heightened identity assurance standard.

***Description of New Emergency Information Collection Tool***

SSA is implementing the new hybrid Security Authentication PIN (SAP) to digitally verify the identity of a telephone respondent or an in-person respondent who lacks identification when requesting changes to their direct deposit information. This supports the agency's changes to its identity proofing policy for direct deposit enrollments, updates or cancellations.

In addition, for circumstances where a respondent is seeking direct deposit requests in-person at a field office and they are required to provide an acceptable form of identification (e.g., State ID/driver's license, U.S. Passport, etc.), the SAP will provide an alternative option for individuals who do not have the requisite identity document with them at the time.

In both scenarios, if the respondent does not have an acceptable form of identification on their person, the technician will ask if the respondent has an online *my* Social Security account. If they do, the technician will provide the respondent with a direct link, either by reading the vanity URL to the respondent or by sending a link via email or text. The respondent can then generate the 8-digit Security Authentication PIN (SAP) after signing into their account. The PIN will be valid for 30 minutes, after which the respondent can generate a new PIN if required.

To ease the burden on respondents, SSA created a vanity URL (a custom, user-friendly shortcut URL that redirects to a longer, often more complex destination URL) that will navigate respondents directly to the Security Settings page within their online *my* Social Security account, allowing them to quickly and easily generate the SAP after accessing their account. This feature will reduce the burden on the respondent to navigate within their online account to the Security Settings pages where they may generate the SAP. The code generates immediately once the respondent selects the "Generate PIN" button.

The process will work as follows:

**For respondents who contact SSA by telephone for direct deposit:**

- Respondents provide their SSN to an SSA technician.

- The technician asks "Do you have a *my* Social Security account?

- If the answer is “Yes”:

    1. The technician will provide the respondent with a direct link to their *my* Social Security account’s security settings, either by reading the vanity URL to the respondent or by sending a link via email or text, where the respondent can generate an 8-digit Security SAP after signing into their account and successfully completing Multifactor Authentication (MFA) through SSA’s current credentialing and authentication process (OMB No. 0960-0789).

    2. The respondent uses the direct link to generate a SAP using the “Generate PIN” button on their *my* Social Security account’s security settings page.

    3. The SAP will be valid for 30 minutes, after which the respondent can generate a new PIN if required.

        - Note: the SAP will override the usage of an established series of identifying questions. Therefore, this new process will not create a change in time or burden for the respondent. However, if the respondent’s request is to change existing bank data, the respondent will still need to answer the additional identifying questions currently required by policy to make changes to existing direct deposit information via the phone service channel (as per the current requirements and burden listed under OMB No. 0960-0634).

    4. The technician then enters the SAP in TED to verify the respondent’s identity.

        - If the SAP matches the information in the system, the technician continues by providing the requested service (e.g. making a payment method change).

        - If the SAP does not match, the technician will ask the respondent to use the “Generate PIN” button to generate a new SAP. Then they will proceed through steps 2-4 again.

- If the answer is “No”:

    1. The technician instructs respondent to create a *my* Social Security account (using Login.gov or ID.me) and requests that the respondent call back once they complete account creation.

        - Note: if the respondent does not wish to create an online Social Security account, the technician directs the respondent to visit their

local field office and present identification in person.

- End Call.

**For Respondents who visit SSA in person to request direct deposit changes but do not have an identity document:**

- The SSA technician requests the respondent's SSN.
- The respondent provides the SSN to SSA Technician.
- The SSA technician requests acceptable forms of identification (e.g., State ID/driver's license, U.S. Passport, etc.).
- If the respondent does not have an acceptable form of identification on their person, the technician will ask if the respondent has an online *my* Social Security account.
    - If the answer is "Yes":
        1. The technician will provide the respondent with a direct link to security settings, either by reading the vanity URL to the respondent or by sending a link via email or text, where they can generate an 8-digit Security Authentication PIN (SAP) after signing into their account and successfully completing Multifactor Authentication (MFA). The PIN will be valid for 30 minutes, after which the respondent can generate a new PIN if required.
        2. The technician will wait (and, if needed assist) the respondent in logging into his or her *my* Social Security account.
        3. The respondent will use the vanity URL to generate the SAP using the "Generate PIN" button on the security settings page.
            - Note: the SAP will override the usage of an established series of identifying questions. Therefore, this new process will not create a change in time or burden for the respondent. However, if the respondent's request is to change existing bank data, the respondent will still need to answer the additional identifying questions currently required by policy to make changes to existing direct deposit information via the phone service channel (as per the current requirements and burden listed under OMB No. 0960-0634).
        4. Technician will enter the SAP in TED to verify respondent's identity.
            - If the SAP matches the information in the system, the technician

continues by providing the requested service (e.g. making a payment method change).

- If the SAP does not match, the technician will ask the respondent to use the "Generate PIN" button to generate a new SAP. Then they will proceed through steps 2-4 again.

- If the answer is "No":

1. The technician instructs respondent to create a *my* Social Security account (using Login.gov or ID.me) and requests that the respondent call back once they complete account creation.

   - Note: if the respondent does not wish to create an online Social Security account, the technician directs the respondent to find their identification documents and then return to the field office to present them in person.

***Information the Security Authentication PIN tool will collect***

While the public-facing SAP tool itself will not collect any information, the process of creating or logging into a *my* Social Security account requires the respondent to submit several pieces of identifying information (such as an email address, a password, selecting a multi-factor authentication method, and completing identity proofing, which entails uploading an ID and taking a "selfie") to both sign up/in using ID.me or Login.gov, and to use the enhanced multi-factor identification tool each time the respondent logs in to the account. We previously obtained OMB approval for the burden associated with the creation of the *my* Social Security account under SSA's Public Credentialing and Authentication Process (OMB No. 0960-0789) which utilizes ID.me and Login.gov for authentication purposes. However, while the creation of a *my* Social Security account is already covered under a separate OMB Control number, this emergency approval is intended to be inclusive of the increased burden associated with either (1) generating a SAP through *my* Social Security to complete the direct deposit transaction over the phone or; (2) traveling to a field office because the respondent is unable to create a *my* Social Security account or otherwise is unable to successfully generate a SAP and is no longer able to complete the direct deposit transaction over the phone as previously described in OMB No. 0960-0634 (Domestic Direct Deposit Application).

Once authenticated through the *my* Social Security Account, the respondent will use the vanity URL to request a SAP code by pressing the "Generate PIN" button which then displays the code on their screen. To utilize the SAP process, the respondent will need to use the vanity URL to log into their existing online Social Security account. Once they are signed in, they will generate the code and read it back to the technician. As mentioned above, respondents without an online Social Security account will need to create one with one of our credential service

providers, ID.me or Login.gov. Respondents who create an online account will have the added benefit of being able to access our popular and convenient secure online services going forward. Once the respondent creates the account, they may generate the SAP code and share it with the technician.

Note: Respondents who are unable or unwilling to utilize the SAP process will still have the option of visiting their local field office to verify their identity in person.

***Psychological Costs:***

We recognize that this enhanced identity proofing process will introduce psychological costs for the respondent:

- **Psychological Cost #1:**
  - Requirement for the Process:
    Respondents will need to use their *my* Social Security Account to generate a SAP prior to conducting business with SSA via telephone or, for some cases, in person.

  - Psychological Cost:
    Respondents may find it to be more stressful, time-consuming, and inconvenient than our prior processes, which may cause them to drop out of the process entirely.

To limit the psychological costs for this process, the technician will be able to explain the new process over the phone. This includes sending the respondent a vanity URL which will take the respondent into the specific settings screen from their online Social Security account where they generate the 8-digit SAP code. Built into this process is the ability for the respondent to generate a second code should the first code they provide to the technician not match, so they may try again without having to recontact the agency. The technician will validate this code when the technician enters it into the TED application. The TED application will respond immediately and will also retain the results of the verification in the digital identity database where the system stores the initial code awaiting systematic verification. The technician can explain to the respondent that these are agency-wide changes to our identification process to prevent fraud and enhance the integrity and security of our records.

The respondents are individuals who wish to do business with SSA over the telephone or in person without identification for the purposes of direct deposit enrollments, updates or cancellations.

**3. Use of Information Technology to Collect the Information**

In accordance with the Government Paperwork Elimination Act, SSA created a one-time-passcode generation tool, as an alternative method to establishing

sufficient identity verification, such as in-person verification of identity documents. As this tool is only available through the respondent's *my* Social Security account, we anticipate that 100 percent of the respondents who use the tool will use the electronic method. However, we anticipate that only up to 50 percent of all respondents who wish to do business with SSA via the telephone or in person will choose to use the electronic code either through their Internet screens or handheld (mobile) device. Members of the public who prefer not to use the one-time-passcode for this information collection, or who do not have access to the Internet, may continue to visit an FO to satisfy the identity verification requirements.

4. **Why We Cannot Use Duplicate Information**
   SSA uses another similar collection instrument, the Elevated Phone Identity Verification (EPIV) tool, available from the Registration and Customer Support (RCS) application and the TED, to verify respondents over the telephone (OMB No. 0960-0789). During the EPIV process, we ask the respondent to provide a self-asserted address or phone number, which we then attempt to verify using internal records, as well as our Identity Services Provider (Experian). If we can verify the respondent's digital (text-enabled cell phone) or physical address, EPIV delivers a one-time use code by mail or text to the respondent's verified text-enabled cell phone number or physical address for the respondent to verbally confirm. EPIV cannot be used to identity proof an individual as part of the credentialing process for the agency's digital services, such as *my* Social Security.

   EPIV was originally designed as an alternative to in-person identity-proofing for targeted workloads (eService block removal and anomalous claims) during the COVID-19 pandemic when in-person services were not available. The agency did not intend to rely upon it as the sole source of identity-proofing for respondents making changes to their record. Additionally, the reliance on a self-asserted address or phone number, even if verified against internal and external records, still leaves open the possibility of a fraudster successfully completing EPIV phone verification by associating a phone number in their possession with an unknowing respondent's Experian record. Requiring the respondent to create or sign into their online *my* Social Security account, generate the code themselves, and then read it to the technician via the SAP process mitigates this risk.

   Therefore, the SAP process is necessary to implement for this purpose, and we cannot use EPIV for these requests.

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**
   Recent changes to SSA's identity verification policy for direct deposit enrollments, updates, and cancellation requests requires additional identity proofing to mitigate fraud concerns.

Respondents will no longer be able to verify their identity over the phone merely by answering a series of knowledge-based questions, rather they will also use a multi-factor authentication using the SAP process. We will require respondents who are unable to use the SAP process to visit their local field office in person to present acceptable identity documents. Traveling to the local field office is an added burden that far exceeds the impact of the generation, communication, and collection of the SAP code. Since we will only collect this information for direct deposit requests, we cannot collect it less frequently. There are no technical or legal obstacles to burden reduction.

**7. Special Circumstances**

There are no special circumstances that would cause SSA to collect this information in a manner inconsistent with *5 CFR 1320.5*.

**8. Solicitation of Public Comment and Other Consultations with the Public**

SSA published this Emergency PRA Approval Request in the *Federal Register* on April 18, 2025, at 90 FR 16583. Due to the critical time sensitivity of this ICR OMB has agreed to allow for a shorter formal public comment period of twenty-one days.

We may initiate a new PRA process and seek public comment in the *Federal Register* prior to the end of the standard 6-month duration of an emergency clearance. We will also consider any comments submitted during the emergency clearance process at that time.

**Consultation with the Public:**

The Acting Commissioner of Social Security met with the advocate community on March 24, 2025 to better understand their concerns with the agency's new identity proofing policy. SSA used this open discussion listening session to hear the advocates concerns regarding fraud mitigation, identity proofing, travel times to field offices and wait times in field offices, and other concerns. The meeting included representatives from several advocacy organizations, including the National Organization of Social Security Claimants' Representatives (NOSSCR), National Association of Disability Representatives (NADR), AARP, the Center for Democracy and Technology, the Advocacy and Training Center, New York Legal Assistance Group, Empire Justice Center, Justice in Aging, Center on Budget and Policy Priorities, Legal Aid of North Carolina, Legal Council for Health Justice, Centauri Health Solutions, Midwest Disability, and several law offices

**9. Payment or Gifts to Respondents**

SSA does not provide payments or gifts to the respondents.

**10. Assurances of Confidentiality**

SSA protects and holds confidential the information it collects 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), and OMB Circular No. A-130.

**11. Justification for Sensitive Questions**

The information collection does not contain any questions of a sensitive nature.

**12. Estimates of Public Reporting Burden**

The chart below shows our estimated burden figures for the respondents to learn about and use the hybrid SAP identity proofing tool. It also includes respondents who drop out of the telephone request and need to request the SAP in a field office. We estimated these figures based on the current volume of claims and direct deposit changes made through the phone modality based on our current management information (MI) data:

| **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 for Teleservice Center or Field Office (minutes)** ** | **Total Annual Opportunity Cost (dollars)***** |
|---|---|---|---|---|---|---|---|
| Member of public requesting phone-based assistance direct deposit assistance via SAP Process | 1,937,000 | 1 | 8+ | 258,267 | $32.66* | 0 | $8,435,000*** |
| Member of public requesting direct deposit who cannot complete over the phone | 1,937,000 | 1 | 2 | 64,567 | $32.66* | 21 | $24,250,605*** |
| Member of the public requesting direct deposit in a field office who needs identity proofing | 1,937,000++ | 1 | 8+ | 258,267 | $32.66* | 23 | $32,685,605*** |
| **Totals** | **5,811,000** | | | **581,101** | | | **$65,371,210***** |

[+] Note: this figure does not include the knowledge-based questions; however, we will use this figure in place of the knowledge-based question figure currently listed under OMB No. 0960-0789 for telephone respondents.

[++] We note that some of these respondents may already have *my* Social Security accounts. For the purposes of this Emergency Clearance, we will assume they need to create an account which is why they needed to go into the field office, and we account for burden to create an account under OMB No. 0960-0789.

* We based this figure on the average U.S. worker's hourly wages, as reported by Bureau of Labor Statistics data (Occupational Employment and Wage Statistics).

** We based this figure on the average FY 2025 combined wait times for teleservice centers and field offices, 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 online tool; rather, these are theoretical opportunity costs for the additional time respondents will spend to complete the tool. **There is no actual charge to respondents to complete the online tool**.

Note: Since the respondents learn about the new hybrid SAP process upon contacting the agency (either via telephone or in person), we included the Learning Cost in the average burden per response listed in the chart above, and we did not calculate a separate learning cost.

In addition, we did not include a separate chart for the Travel Time burden, as we already account for this burden under OMB No. 0960-0789, and we do not want to double-count it here.

We base our burden estimates on Fiscal Year 2024 MI data for direct deposit changes made through the phone contact method. Per our MI data, we believe that **8** minutes accurately shows the average burden per response for learning about the program; receiving 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 MI data, the current burden information we provided is accurate. The total burden for this ICR is **581,101** burden hours (reflecting SSA MI data), which results in an associated theoretical (not actual) opportunity cost financial burden of **$63,262,420**. SSA does not charge respondents to complete our applications.

**13. Annual Cost to the Respondents (Other)**

This collection does not impose a known cost burden on the respondents.

**14. Annual Cost to Federal Government**

The annual cost to the Federal government is approximately $**1,168,709,600**. This estimate accounts for costs from the following areas:

| **Description of Cost Factor** | **Methodology for Estimating Cost** | **Cost in Dollars*** |
|---|---|---|
| Designing the Collection | Design Cost + Printing Cost | $0* |
| Distributing, Shipping, and Material Costs for the Collection | Distribution + Shipping + Material Cost | $0* |
| SSA Employee (e.g., field office, 800 number, DDS staff) Information Collection and Processing Time | SSA employees, 1,937,000 x 16 minutes for successful (both on the phone and in office); 1,937,000 x 2 minutes for unsuccessful | $1,168,011,000 |
| Full-Time Equivalent Costs | Out of pocket costs + Other expenses for providing this service | $0* |
| Systems Development, Updating, and Maintenance | SSA employees for development, updating, maintenance | Development: $577,467<br><br>Annual Maintenance: $113,896 |
| Quantifiable IT Costs (UXG support) | Any additional IT costs | $7,237 |
| **Total** | | **$1,168,709,600** |

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

SSA is unable to break down the costs to the Federal government further than we already have. It is difficult for us to break down the cost for processing a single form, as field office and State Disability Determination Services staff often help respondents fill out several forms at once, and the time it takes to do so can vary greatly per respondent. As well, because so many employees have a hand in each aspect of our forms, we use an estimated average hourly wage, based on the wage of our average field office employee (GS-9) for these calculations. However, we have calculated these costs as accurately as possible based on the information we collect for creating, updating, and maintaining these information collections.

**15. Program Changes or Adjustments to the Information Collection Request**

This is a new Internet-based tool that increases the public reporting burden. See question #12 above for updated burden figures.

* Note: The total burden reflected in ROCIS is **2,001,567**, while the burden cited

in #12 of the Supporting Statement is **581,101**. This discrepancy is because the ROCIS burden reflects the average teleservice center and field office waiting times as well as the burden per response. In contrast, the chart in #12 of the Supporting Statement reflects actual burden.

**16. Plans for Publication Information Collection Results**

SSA will not publish the results of the information collection.

**17. Displaying the OMB Approval Expiration Date**

SSA is not requesting an exception to the requirement to display the OMB approval expiration date.

**18. Exceptions to Certification Statement**

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

## B. Collections of Information Employing Statistical Methods

SSA does not use statistical methods for this information collection.