

The Exchange does not believe the proposed rule change to adopt Extended Trading Hours will impose an undue burden on inter-market competition because the proposed rule change is a competitive initiative that will benefit the marketplace and investors. The Exchange believes that the proposed rule change enhances competition by providing a service to investors that only a small number of options exchanges currently provide.⁴⁵ Additionally, all options exchanges are free to compete in the same manner. The Exchange further believes that the same level of competition among options exchanges will continue during Regular Trading Hours. The Exchange also believes that the proposed rule change could increase its competitive position outside of the United States by providing investors with an additional investment vehicle with respect to their global trading strategies during times that correspond with parts of regular trading hours outside of the United States.

C. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received From Members, Participants, or Others

No written comments were either solicited or received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the **Federal Register** or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the Exchange consents, the Commission will:

- A. by order approve or disapprove such proposed rule change, or
- B. institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views, and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's internet comment form (<https://www.sec.gov/rules/sro.shtml>); or

- Send an email to rule-comments@sec.gov. Please include file number SR-MRX-2026-11 on the subject line.

Paper Comments

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090. All submissions should refer to file number SR-MRX-2026-11. This file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's internet website (<https://www.sec.gov/rules/sro.shtml>). Copies of the filing will be available for inspection and copying at the principal office of the Exchange. Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to file number SR-MRX-2026-11 and should be submitted on or before April 21, 2026.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.⁴⁶

Sherry R. Haywood,
Assistant Secretary.

[FR Doc. 2026-06153 Filed 3-30-26; 8:45 am]

BILLING CODE 8011-01-P

SOCIAL SECURITY ADMINISTRATION

[Docket No: SSA-2026-0331]

Agency Information Collection Activities: Comment Request

The Social Security Administration (SSA) publishes a list of information collection packages requiring clearance by the Office of Management and Budget (OMB) in compliance with Public Law 104-13, the Paperwork Reduction Act of 1995, effective October 1, 1995. This notice includes a revision of an OMB-approved information collection.

SSA is soliciting comments on the accuracy of the agency's burden estimate; the need for the information; its practical utility; ways to enhance its quality, utility, and clarity; and ways to minimize burden on respondents, including the use of automated collection techniques or other forms of information technology. Mail, email, or

fax your comments and recommendations on the information collection to the OMB Desk Officer and SSA Reports Clearance Officer at the following addresses or fax numbers.

(OMB) Office of Management and Budget, Attn: Desk Officer for SSA.
(SSA) Social Security Administration, OLC/A, Attn: Reports Clearance Director, Mail Stop 3253 Altmeyer, 6401 Security Blvd., Baltimore, MD 21235, Fax: 833-410-1631, Email address: OR.Reports.Clearance@ssa.gov.

Or you may submit your comments online through <https://www.reginfo.gov/public/do/PRAmain> by clicking on Currently under Review—Open for Public Comments and choosing to click on one of SSA's published items. Please reference Docket ID Number [SSA-2026-0331] in your submitted response.

SSA submitted the information collection below to OMB for clearance. Your comments regarding this information collection would be most useful if OMB and SSA receive them 30 days from the date of this publication. To be sure we consider your comments, we must receive them no later than April 30, 2026. Individuals can obtain copies of this OMB clearance package by writing to the OR.Reports.Clearance@ssa.gov.

mySocial Security—Security Authentication PIN—20 CFR 401.45—0960-0846

In March 2025, SSA announced that new measures were being implemented to enhance security through stronger identity verification procedures. As initially announced, the new procedures were to apply to all benefit claims and direct deposit changes, for which customers would need to use their *my* Social Security account (with online identity proofing) or visit an office to prove their identity in person. In other words, once the new measures were implemented, new benefit claims and direct deposit changes could no longer be completed over the telephone. In response to feedback from customers, Congress, advocates and others, SSA revised this plan several times after it was first announced. Today (and since at least July 2025), the enhanced identity verification procedures apply only to direct deposit changes; and using the Security Authentication PIN process described herein, customers can still make direct deposit changes over the telephone.

To support these enhanced identity proofing measures, in April 2025, SSA published an Emergency Request FRN on April 18, 2025, at 90 FR 16583, then, upon OMB's approval of the Emergency Clearance, implemented a hybrid

⁴⁵ See *supra* note 8.

⁴⁶ 17 CFR 200.30-3(a)(12).

identity proofing process called the *my* Social Security—Security Authentication PIN (SAP) that provides identity proofing parity with our online and in-person modalities. Utilizing the SAP process provides the necessary identity verification to allow direct deposit changes via phone, while ensuring fraud protection through stronger verification of the identity of the individual prior to accessing or revising their account.

OMB granted an Emergency approval for the *my* Social Security—Security Authentication PIN (SAP) collection. We are publishing this 30-day comment period Notice to initiate the full information collection request renewal for the SAP process. We received public comments on the Emergency FRN and on the 60-day comment period FRN which we addressed within the documentation for the full renewal.

Background

Our prior telephone process for direct deposit required respondents to use knowledge-based questions and match information in SSA's records to verify their identity. Knowledge-based identity verification methods are susceptible to compromise by bad 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 direct deposit changes to be a higher risk task meriting a heightened identity assurance standard. To ensure that higher level of identity verification, we instituted the SAP process to ensure higher security for the submission of financial data to SSA over the telephone.

We continue to offer other ways to make direct deposit changes including in-person at a field office; online through *my* Social Security; and automated enrollment through the customer's bank.

Description of the Security Authentication PIN (SAP) Process

SSA's hybrid Security Authentication PIN (SAP) digitally verifies the identity of a telephone respondent (whether a beneficiary or recipient, or his or her representative payee) over the phone with an SSA technician. In addition, for circumstances where a respondent is seeking direct deposit requests in-person at a field office and he or she is required to provide an acceptable form of identification (e.g., State ID/driver's license, U.S. Passport, etc.), the SAP provides an alternative option for individuals who do not have the

requisite identity document with them at the time.

When respondents call SSA to request a change to their direct deposit, the automated telephone system informs them that they will have to log into their *my* Social Security accounts to request a SAP code before they are automatically placed in a dedicated call back queue. Once added to the dedicated callback queue, the next available technician places an outbound call to the respondent and, upon connecting with the respondent, asks if the respondent has a *my* Social Security account. If the respondent does, the technician asks him or her to log into the account through a dedicated vanity URL link (www.ssa.gov/pin), or sends the link to the respondent via email or text message so that the respondent may authenticate using their online account and generate an eight-digit SAP. SSA created the user-friendly vanity URL (a custom, short-cut URL) that navigates respondents directly to the SAP generation page, allowing them to quickly and easily generate the SAP after accessing their account to ease the burden on customers. This feature reduces the burden on the respondent to navigate within his or her online account, authenticate, and generate the SAP. Once created, the SAP is valid for three hours and generates immediately when the respondent selects "Generate PIN" from the link the technician provides. There is no limit to the number of SAPs a customer can generate during a single transaction.

The process works as follows:

For first or third party (individual representative payees requesting post-entitlement direct deposit actions) respondents who contact SSA by telephone:

- Upon connecting with our automated telephone system, the system asks the respondent to give the reason for his or her call. If he or she responds by requesting a change to his or her direct deposit, the system informs the respondent that he or she must first generate a secure, one-time code by going to ssa.gov/PIN and reminds the respondent that he or she can also make these updates using either their secure *my* Social Security account or by contacting his or her financial institution. Following these instructions, the system informs the caller that he or she will receive a callback and will have the opportunity to update the phone number we use to contact him or her.

- The system then adds the caller to the dedicated callback queue. Once added to the dedicated callback queue, the next available technician places an

outbound call to the respondent and, upon connecting with the respondent, asks if he or she has a *my* Social Security account.

- If the answer is "Yes":

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

- The respondent uses the direct link to generate a SAP using the "Generate PIN" button on his or her *my* Social Security account SAP page.

- The SAP code is valid for three hours, so if the callers are disconnected, they can still use this SAP within the three-hour period. The respondents can generate a new SAP at any time.

- **Note:** Generating the SAP allows the respondents to safely complete their direct deposit changes over the telephone and replaces the need for the respondents to either complete their direct deposit changes in person or through a *my* Social Security account. Since the SAP process takes about the same time as logging into a *my* Social Security account, it does not change the time burden for the respondents.

- The respondent provides the SAP to the technician and the technician enters the SAP in TED to verify the respondent's identity.

- If the SAP matches the information in the system, the call continues, and the respondent can make direct deposit changes via telephone.

- If the SAP does not match, the technician requests the respondent generate a new SAP and attempt to verify again. If the respondent is unable to verify the SAP, the technician informs the respondent that he or she will need to either complete the direct deposit change request through his or her *my* Social Security account; ask his or her bank to make the change through the Automated Enrollment (ENR) process; or offers an appointment for an in-person visit to a field office to complete the direct deposit changes.

- If the answer is "No.":

- The technician informs the respondents that he or she will need to either complete the direct deposit request through his or her *my* Social Security account; ask his or her bank to make the change through the Automated Enrollment (ENR) process; or offers him or her an appointment for an in-person visit to a field office to complete the direct deposit changes.

- End call.

○ **Note:** Organizational Payees maintain their ability to add, change, or remove direct deposit or direct express information as they have previously and continue to operate outside of the SAP process. We only require individual representative payees who are not Organizational Payees to complete the SAP process on their own behalf to establish their identities with SSA before making direct deposit changes on behalf of the claimant they are representing.

For Respondents who visit SSA in person to request direct deposit changes but do not have the necessary identity document(s) to authenticate themselves:

- The technician requests the respondent's SSN.
- The respondent provides the SSN to technician.
- The 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 his or her person, the technician asks if the respondent has an online *my* Social Security account. If he or she does, the technician asks if he or she wants to generate a SAP code.
 - If the answer is "Yes":
 - The technician provides the respondent with a direct link to the SAP screen, 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 Authentication PIN (SAP) after the respondent signs into his or her *my* Social Security account and successfully completes Multifactor Authentication (MFA). The SAP is valid for three hours. The respondent can generate a new SAP at any time, if required.
 - The technician waits (and, if needed assists) the respondent in logging into his or her *my* Social Security account.
 - The respondent uses the vanity URL to generate the SAP using the "Generate PIN" button from within the *my* Social Security account.
 - **Note:** The SAP replaces the need for respondents to submit their identifying documents in person. Therefore, the SAP

process does not change the time burden for the respondents.

- The technician enters 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 direct deposit changes (e.g., making a payment method change).
 - If the SAP does not match, the technician asks the respondent to use the "Generate PIN" button to generate a new SAP. Then the technician helps the respondent proceed through steps 2–4 again.
 - If the SAP does not match the second time, the technician helps the respondent set up a second in-person appointment with a reminder to bring identifying documents to that appointment and reminds the respondent that he or she can ask the bank to make the change through the Automated Enrollment (ENR) process.
 - If the answer is "No":
 - The technician helps the respondent set up a second in-person appointment with a reminder to bring identifying documents to that appointment.

Information the Security Authentication PIN Tool Will Collect

While the public-facing SAP tool itself does 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/or use *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, we are accounting for the increased burden associated with generating a SAP through *my* Social Security to complete a direct deposit transaction with SSA over the telephone.

For Respondents, or their Representative Payees, who cite a dire need situation to conduct business over the phone for Direct Deposit (who are unable to generate the SAP or visit a field office):

For respondents meeting certain dire need criteria, SSA may permit respondents to make direct deposit changes by telephone without SAP authentication. Respondents meeting the exception criteria are identified through a personal interview with a technician using Form SSA–553, Special Determination. The technician initiates the exception process during the interview for the SAP process if the respondent is unable to complete the SAP process or visit a field office due to severe restrictions. In those cases, the SSA technician, or SSA management, completes the fillable PDF version of the SSA–553 during the personal telephone interview. The technician then submits the completed SSA–533 to SSA management who reviews the request and decides whether to grant the exception based on the information provided. If management grants the exception, the respondent uses knowledge-based verification over the phone prior to completing his or her direct deposit changes (the same verification we use for our other telephone services). Since this process is less effective in mitigating fraud and securing financial information, SSA limits the use of this request to dire need situations. SSA technicians determine dire need on a case-by-case basis.

The respondents are individuals who wish to do business with SSA over the telephone or in person for the purpose of direct deposit enrollments, updates or cancellations.

Type of Request: Revision of an OMB-approved information collection.

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 and teleservice centers (minutes) **	Total annual opportunity cost (dollars) ***
Respondents requesting phone-based assistance changes for direct deposit using the SAP process	528,626	1	5	44,052	* \$23.47	** 6	*** \$2,274,595
Respondents requesting changes for direct deposit who failed SAP over the phone	+26,343	1	4	1,756	* 23.47	** 6	*** 103,033
Respondents requesting direct deposit who chose to visit a field office who need identity proofing via SAP	++ 395	1	5	33	* 23.47	** 23	*** 4,318

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 and teleservice centers (minutes)**	Total annual opportunity cost (dollars)***
Respondents who drop out of SAP and use an alternate method for changing direct deposit.***	2,084,532	1	9	312,680	* 23.47	** 23	*** 26,092,796
Totals	2,639,896			358,521			*** 28,474,742

* **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 information collection, 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.

*** All of our methods for direct deposit changes are OMB approved; therefore, we do not account for any additional burden here.

* We based this figure by averaging both the average DI payments based on SSA's current FY 2026 data (Effect of COLA on Average Social Security Benefits), and 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 2026 wait times for the teleservice centers and dedicated direct deposit queues (telephone and field office), 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.*

Dated: March 27, 2026.

Mark Steffensen,

General Counsel, Chief of Law and Policy,
Social Security Administration.

[FR Doc. 2026–06182 Filed 3–30–26; 8:45 am]

BILLING CODE 4191–02–P

DEPARTMENT OF STATE

[Public Notice: 12981]

30-Day Notice of Proposed Information Collection: Technology Security/Clearance Plans, Screening Records, and Non-Disclosure Agreements Pursuant to 22 CFR 126.18

ACTION: Notice of request for public comment and submission to OMB of proposed collection of information.

SUMMARY: The Department of State has submitted the information collection described below to the Office of Management and Budget (OMB) for approval. In accordance with the Paperwork Reduction Act of 1995 we are requesting comments on this collection from all interested individuals and organizations. The purpose of this Notice is to allow 30 days for public comment.

DATES: Submit comments up to April 30, 2026.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under 30-day Review—Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: Direct requests for additional information regarding the collection listed in this notice, including requests for copies of the proposed collection

instrument and supporting documents, Andrea Battista, who may be reached at battistaal@state.gov via email and 202–992–0973 via phone.

SUPPLEMENTARY INFORMATION:

- *Title of Information Collection:* Technology Security/Clearance Plans, Screening Records, and Non-Disclosure Agreements Pursuant to 22 CFR 126.18(c)(2).

- *OMB Control Number:* 1405–0195.
- *Type of Request:* Extension of Currently Approved Collection.
- *Originating Office:* Bureau of Political-Military Affairs, Directorate of Defense Trade Controls (PM/DDTC).
- *Form Number:* No form.
- *Respondents:* Business and Nonprofit Organizations.
- *Estimated Number of Respondents:* 10,000.
- *Estimated Number of Responses:* 10,000.
- *Average Time per Response:* 10 hours.
- *Total Estimated Burden Time:* 100,000 hours.
- *Frequency:* On occasion.
- *Obligation to Respond:* Mandatory.

We are soliciting public comments to permit the Department to:

- Evaluate whether the proposed information collection is necessary for the proper functions of the Department.
- Evaluate the accuracy of our estimate of the time and cost burden for this proposed collection, including the validity of the methodology and assumptions used.
- Enhance the quality, utility, and clarity of the information to be collected.
- Minimize the reporting burden on those who are to respond, including the use of automated collection techniques or other forms of information technology.

Please note that comments submitted in response to this Notice are public record. Before including any detailed

personal information, you should be aware that your comments as submitted, including your personal information, will be available for public review.

Abstract of Proposed Collection

The export, temporary import, and brokering of defense articles, defense services, and related technical data are licensed by the Directorate of Defense Trade Controls (DDTC) in accordance with the International Traffic in Arms Regulations (“ITAR,” 22 CFR parts 120–130) and Section 38 of the Arms Export Control Act (“AECA”).

ITAR § 126.18 eliminates, subject to certain conditions, the requirement for an approval by DDTC of the transfer of unclassified defense articles, which includes technical data, to or within a foreign business entity, foreign governmental entity, or international organization that is an authorized end-user or consignee (including transfers to approved sub-licensees) for defense articles, including the transfer to dual nationals or third-country nationals who are bona fide regular employees directly employed by the foreign consignee or end-user.

To use ITAR § 126.18, effective procedures must be in place to prevent diversion to any destination, entity, or for purposes other than those authorized by the applicable export license or other authorization. Those conditions can be met by requiring a security clearance approved by the host nation government for its employees, or by the end-user or consignee having in place a process to screen all its employees and to have executed a Non-Disclosure Agreement that provides assurances that the employee will not transfer any defense articles to persons or entities unless specifically authorized by the consignee or end-user. ITAR § 126.18(c)(2) also provides that the technology security/clearance plans and screening records shall be made available to DDTC or its