APPLICATION FOR ACCESS TO SSA SYSTEMS

(TYPE OR PRINT CLEARLY- ALL ILLEGIBLE FORMS WILL BE RETURNED)

1. Applicant Information	2. Type of Request
☐ SSA Employee ☐ Non SSA Employee (Please specify) SEE INSTRUCTIONS	(Please enter all previous issued PINS/TSO IDs) ☐ 2A. Create New ☐ 2B. Change Access/LOC/ORG ☐ PIN PIN ☐ TSO ID TSO ID
3A. Environment For Access (Check only one) ☐ Production ☐ Integration ☐ LAN Only ☐ ESEF (Complete block 3B)	3B. ESEF only (Check all that apply) ☐ ESEF TSO/BATCH ☐ ESEF CICS TEST ☐ ESEF CICS VALIDATION

4. (PRINT) Last Name	First (Official)	MI	5. Social Security Number	6. Office/Branch Code

7. SSA Component and Security Department or External Organization	8. Position Title (See Instructions)

9. Justification/Remarks

10. I have read and understand the security requirements and privacy act statement on page 2 of this form. ☐ See continuation sheet

11A. Applicant's Signature	11B. Date	11C. Telephone

RESERVED FOR REQUESTOR'S MANAGEMENT AUTHORITY

12A. (PRINT) Requestor's Management Official's Name	12B. Requestor's Management Official's Signature

12C. Title	12D. Telephone	12E. Requestor's Mailing Address	12F. Date

RESERVED FOR REVIEWING SECURITY AUTHORITY

13A. (PRINT) Reviewing Security Official's Name CDSI/CSO	13B. Reviewing Security Official's Mailing Address
13C. Reviewing Security Official's Signature	

13D. Date	13E. Telephone	13F. Component/Region

RESERVED FOR FINAL APPROVING AUTHORITY

14A. (PRINT) Approving Official's Name	14B. Approving Official's Signature	
14C. Title	14D. Telephone	14E. Date

14F. Date Received	14G. PIN/TSO ID	14H. Base Profile

14I. PIN/TSO ID Expires:	15. If you have any questions, contact:

☐ 16. Access Denied
(Reason)

SECURITY REQUIREMENTS FOR USERS OF SSA'S COMPUTER SYSTEMS

You should be aware that your PIN/ID serves as your "electronic signature" on all systems transactions for which it is used. This means that you will be held responsible if someone else uses it in connection with a systems transaction.

To monitor the users of SSA's computer systems for compliance with these requirements, SSA records all systems transactions and conducts routine reviews for inappropriate or illegal activity.

A violation of any of the following security requirements could result in termination of systems access privileges and serious disciplinary action, possibly removal. In addition, Public Law 98-473, Chapter 21 ("Counterfeit Access Device and Computer Fraud and Abuse Act of 1984"), and Public Law 99-474 ("Computer Fraud and Abuse Act of 1986") provide criminal penalties for any person accessing a Government-owned or operated computer illegally.

The information below will assist you in carrying out your responsibility in this area.

1. The PIN/ID you are assigned is for your use only. Lending it to someone else is a security violation and may result in disciplinary action against both parties.

2. Never disclose your password. Do not put it in writing. Safeguard it. Your password is the key to one of SSA's most valuable resources.

3. SSA's computer systems must be used only for work-related purposes which are consistent with the justification on each user's approved request for systems access privileges. Never use the Agency's computers for activities inconsistent with SSA's mission.

If you become aware of any violation of these requirements or suspect that your PIN/ID may have been used by someone else, it is your responsibility to immediately report that information to your security officer.

Privacy Act Statement
Collection and Use of Personal Information

Section 205(a) of the Social Security Act, as amended, 5 U.S.C. § 552a(e)(10), and 44 U.S.C. § 3553 allow us to collect this information. Furnishing us this information is voluntary. However, failing to provide all or part of the information may affect your ability to access the agency's information technology systems and resources.

We will use the information to authorize access to the agency's information technology systems. We may also share your information for the following purposes, called routine uses:

- To notify another Federal agency when, or verify whether, a Personal Identity Verification card is no longer valid; and

- We may disclose information to appropriate Federal, State, and local agencies, entities, and persons when (1) we suspect or confirm that the security or confidentiality of information in this system of records has been compromised;(2) we determine that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs of Social Security Administration (SSA) that rely upon the compromised information; and(3) we determine that disclosing the information to such agencies, entities, and persons is necessary to assist in our efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. SSA will use this routine use to respond only to those incidents involving an unintentional release of its records.

In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of additional routine uses is available in our Privacy Act System of Records Notices (SORN) 60-0214, entitled Personal Identification Number File, as published in the Federal Register (FR) on September 8, 1994, at 59 FR 46439, and 60-0361, entitled Identity Management System, as last published in the FR in full on November 3, 2006, at 71 FR 64751, and subsequently modified on December 10, 2007, at 72 FR 69723. Additional information and a full listing of all our SORNs are available on our website at www.ssa.gov/privacy/.

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 0960-0791. We estimate that it will take about 2 minutes to read the instructions, gather the facts, and answer the questions. ***Send only comments relating to our time estimate above to*****:** *SSA*, *6401 Security Blvd, Baltimore, MD 21235-6401.*

INSTRUCTIONS FOR COMPLETING THE APPLICATION FOR ACCESS TO SSA- SYSTEMS (SSA-120)

1.	Applicant Information	For non-SSA employees please specify whether you are a contractor, DDS, Host enrollee, Student, etc. See ISP Section: Access Control for additional details.
2.	Type of request	• If you do not have a PIN or TSO ID and need one assigned place an “X” in the appropriate box(es). • If you have a PIN/TSO ID but need your access privileges, location or organization changed place an “X” in the appropriate box(es).
3. A.	Environment for access	Place one “X” in the box to indicate what environment you require access to. If you are applying for ESEF access complete box 3B. If you are not applying for ESEF skip 3B.
3. B.	SEF environment	Place an “X” in all applicable boxes for ESEF environment.
4.	Name	Print official name as in personnel records (no nicknames).
5.	Social Security Number	Provide the SSN of the person applying for PIN/TSO ID.
6.	Office/Branch Code	Provide the 3-digit office code if you are requesting a PIN. Provide the 3 digit branch code if you are requested the creation of a TSO ID.
7.	SSA Component and Security Department or External Organization	SSA Field employees should enter the name of their Field office and Security Department. SSA non-field office employees should enter their component name and Security Department. All others enter the name of your employing company or agency. Security Department example: **Dept: DOISDSE.**
8.	Position Title	• SSA employees – Enter your position title from your most recent SF-50, Notification of Personnel Action. Claims representatives must also enter their specialty. • Non SSA employees – Enter the title commonly used by your company or organization for your position.
9.	Justification/Remarks	Use this space to justify access privileges needed. If your access is needed for a specific project or domain provide the information.
10.	Security Requirements and Privacy Act Statement	
11. A.	Applicant’s Signature	After reading the Security Requirements and Privacy Act Statement in Block 10, signature of person named in Block 4 should be provided.
11. B.	Date	Enter date when signature provided in Block 11. A.
11. C.	Telephone Number	Provide work telephone number including area code for the person in Block 11. A.
12. A.	Requesting Management Official’s Name	A Division Director or higher-level official within the requesting component must approve and sign the form for personnel in central office components.
12. B.	Requesting Management Official’s Signature	Provide signature of person named in Block 12. A.
12. C.	Title	Provide the title of the person named in Block 12. A.
12. D.	Telephone Number	Provide work telephone number including area code for the person in Block 12. B.
12. E.	Requesting Management Official’s Mailing Address	Provide mailing address of person named in Block 12. A.
12. F.	Date	Enter date when signature provided in Block 12. B.
13. A.	Print Reviewing Security Official’s Name CSO/CDSI	Provide printed name of the Reviewing Security Official. If you are the security administrator granting or denying the access skip 13. A-F. Complete your information in section 14 – 16.
13. B.	Reviewing Security Official’s Mailing Address	Provide mailing address for person named in Block 13. A.
13. C.	Reviewing Security Official’s Signature	Signature of person named in Block 13. A. should be entered in this block.
13. D.	Date	Enter date when signature provided in Block 13. C.
13. E.	Telephone Number	Provide work telephone number including area code for the person in Block 13. A.
13. F.	Component/Region	Provide component/region for person named in Block 13. A.
14. A.	Print Approving Official’s Name	Provide printed name of the security administrator granting or denying the access of applicant.

INSTRUCTIONS FOR COMPLETING THE APPLICATION FOR ACCESS TO SSA- SYSTEMS (SSA-120)

14. B.	Approving Official's Signature	Signature of the person named in Block 14. A. should be entered in this block.
14. C.	Title	Provide the title of the person named in Block 14. A.
14. D.	Telephone Number	Provide work telephone number including area code for the person in Block 14. A.
14. E.	Date	Enter date when signature provided in Block 14. B.
14. F.	Date Received	Enter date form was received by the person named in Block 14. A.
14. G.	PIN/TSO ID	Enter the PIN/TSO ID created for the person named in Block 4.
14. H.	Base Profile	Enter the profile given to the person named in Block 4.
14. I.	PIN/TSO ID	Enter expires date for PIN/TSO ID expiration if applicable.
15.	Questions	Enter the name and telephone number including the area code of the person to call if there are any questions.
16.	Access Denied	Enter the reason for denying the access for the person named in Block 4.

Disposition of the Completed Form

1. Regional, Field and DDS personnel – Send the form through the Local Security Officer to the appropriate Security Specialist or Regional Security Officer.

2. Office of Hearing Operations Regional and Field personnel - Send the form through the Security Officer in the OHO Regional Office to the Component Security Officer, 5107 Leesburg Pike, Falls Church, Virginia 22041-3255.

3. For access to the ESEF - Component Security Officer (CSO) should send the signed/ complete form to: OSA Component Security Officer, 3G6D Perimeter East Building.

4. Other Central Office personnel – Send the form through the appropriate Component Security Officer for processing.