SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST
☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☒ USER ID DOD ID number (on CAC)

DATE *(YYYYMMDD)*

SYSTEM NAME *(Platform or Applications)*
iPERMS

LOCATION *(Physical Location of System)*
Ft Knox, KY

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*
SOLDIER, JOE I

2. ORGANIZATION
YOUR ORGANIZATION (DIV/BDE/BN)

3. OFFICE SYMBOL/DEPARTMENT
YOUR PARENT UIC

4. PHONE *(DSN or Commercial)*
YOUR OFFICE NUMBER

5. OFFICIAL E-MAIL ADDRESS
YOUR ENTERPRISE EMAIL ADDRESS ONLY

6. JOB TITLE AND GRADE/RANK
YOUR JOB TITLE/GRADE/RANK

7. OFFICIAL MAILING ADDRESS
YOUR OFFICIAL WORK ADDRESS

8. CITIZENSHIP
☐ US ☐ FN ☐ OTHER

9. DESIGNATION OF PERSON
☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* _____

11. USER SIGNATURE
USER SIGNATURE DIGITALLY OR HAND

12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR*(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS
**********THE BELOW MUST BE ON YOUR DD 2875 THAT YOU SEND REQUESTING ACCESS**********
ACCEPTABLE USE STATEMENT
Personally Identifiable Information (PII) contained in iPERMS is not for public use or access. All functions or actions in iPERMS are tracked by audit logs and can be made available to management upon an official request. Unauthorized disclosure of PII or viewing a Soldier's AMHRR for other than official duty purposes are violations of the Privacy Act which may subject users to civil and criminal penalties. Soldiers that suspect unauthorized use or viewing of their records can request an investigation through their chain of command or local Inspector General. Misuse of PII is a violation of access and can result in the removal of iPERMS access. Examples of PII violations are:
a. Viewing or downloading a Soldier's AMHRR without a mission requirement (e.g. public notoriety or co-workers).
b. Accessing PII for the purpose of identity theft or other criminal misuse.

**********PLEASE SEE PAGE 2 BLOCK 27 FOR REQUIRED INFORMATION**********

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER BLOCKS 17-20b MUST BE COMPLETED/BLOCKS 21-25 ONLY FOR NG

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. ☐

16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*
MUST BE E7/GS11 OR HIGHER

18. SUPERVISOR'S SIGNATURE

19. DATE *(YYYYMMDD)*

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT
ASSIGNED UNIT & GRADE OF SUPERVISOR

20a. SUPERVISOR'S E-MAIL ADDRESS
SUPERVISOR OFFICIAL EMAIL

20b. PHONE NUMBER
000-000-0000

21. SIGNATURE OF INFORMATION OWNER/OPR

21a. PHONE NUMBER

21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE

23. ORGANIZATION/DEPARTMENT

24. PHONE NUMBER

25. DATE *(YYYYMMDD)*

26. NAME *(Last, First, Middle Initial)*

SOLDIER, JOE I

27. OPTIONAL INFORMATION *(Additional information)*

**********THE FOLLOWING INFORMATION IS MANDATORY FOR iPERMS ACCESS**********

1. DETAILED JUSTIFICATION WHY YOU NEED IPERMS ACCESS:

2. YOUR ASSIGNED UNIT/COMMAND UIC: (LIST ALL UIC's OF WHICH VIEWING ACCESS IS REQUIRED)
Please also indicate if the UICs are Active Army or Reserve Command UICs

3. YOUR Enterprise Email ID: (This is the characters in your email address before the .mil@mail.mil, .civ@mail.mil, .ctr@mail.mil)

4. The below training has to be completed 1 time and does not have to be renewed annually
   A. AUTHORIZED OFFICIAL COMPLETION DATE:
   B. SCAN OPERATOR COMPLETION DATE:
   C. RECORD MANAGER COMPLETION DATE:
   Training site for web based training can be found at https://ipermstraining.carson.army.mil/wbt

5. Below training must be completed annually
   D. CYBERAWARENESS CHALLENGE (formally IA) https://ia.signal.army.mil (PUT TRAINING DATE IN BLOCK 10 PAGE 1)
   E. HIPAA CERTIFICATION DATE (Required only if requesting access as "qualified official" to medical documents). Your Certificate of Completion must be sent with your DD 2875.

6. If you are a MEMBER of a USAR unit or work as a Civilian in a USAR unit, your completed form must be sent to your Command's Domain Administrator (formally MPOC) for their action. The below statement MUST be on your DD 2875:

AS THE RESERVE DOMAIN ADMINISTRATOR I HAVE REVIEWED THIS IPERMS APPLICATION AND I RECOMMEND ACCESS TO COMMAND RULE _____ DOMAIN ADMINISTRATOR SIGNATURE & EMAIL ADDRESS_____

1 June 16

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)* 20150902

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(5)Official E-mail Address. The user's official e-mail address.

(6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(7) Official Mailing Address. The user's official mailing address.

(8) Citizenship (US, Foreign National, or Other).

(9) Designation of Person (Military, Civilian, Contractor).

(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.