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	USER ID	DATE *(YYYYMMDD)*

SYSTEM NAME *(Platform of Applications)* □ TC-AIMS II □ AALPS □ AMFT-ITV	LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN and/or Commercial)*	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP	9. DESIGNATION OF PERSON

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

□ I have completed Annual Information Awareness Training. COMPLETION DATE *(YYYYMMDD)*

11. USER SIGNATURE OR UAM SIGNATURE FOR DEACTIVATION	12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER'S SUPERVISOR/UAM OR GOVERNMENT SPONSOR *(If individual is a contractor - provide Company Name and Contract Number in Block 13, and date of contract expiration in Block 16a.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:

15. USER REQUIRES ACCESS TO:

(If Classified or Other is selected, please specify)

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. □	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name and Contract Number in Block 13.)*

17. SUPERVISOR/UAM NAME *(Print Name)*	18. SUPERVISOR/UAM E-MAIL ADDRESS	19. DATE *(YYYYMMDD)*
20. SUPERVISOR/UAM ORG/DEPT	20a. SUPERVISOR/UAM SIGNATURE	20b. PHONE NUMBER
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)*

27. ACCESS REQUEST INFORMATION

ADD Access

Unit Name: ____________ **Assigned UIC:** ____________ **Responsible UIC:** ____________

Preference UICs: ________ ________ ________ ________ ________ ________ ________ ________

Preference Job#: ________ ________ ________ ________ ________ ________ ________ ________

Primary Job Role(s): □ **UMO** □ **UMC** □ **ITO** □ **BMCT** □ **MCE** □ **Mode Oper.**

□ **Mode Mgr.** □ **TTP/MP Mgr.** □ **CoC Mgr.** □ **UAM** □ **DMC** □ **Read Only**

REMOVE Access

Unit Name: ____________ **Assigned UIC:** ____________ **Responsible UIC:** ____________

Preference UICs: ________ ________ ________ ________ ________ ________ ________ ________

Preference Job#: ________ ________ ________ ________ ________ ________ ________ ________

Primary Job Role(s): □ **UMO** □ **UMC** □ **ITO** □ **BMCT** □ **MCE** □ **Mode Oper.**

□ **Mode Mgr.** □ **TTP/MP Mgr.** □ **CoC Mgr.** □ **UAM** □ **DMC** □ **Read Only**

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	
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 SIGNED *(YYYYMMDD)*
DATE PROCESSED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE SIGNED *(YYYYMMDD)*

DD FORM 2875 INSTRUCTIONS

Always use the <TAB> key to advance to the next field.

REQUEST DETAIL:

Type of Request. Choose either Initial, Modification, Deactivate, or Activate.

Date. Date of request.

System Name. Application platform to be initiated, modified or deactivated.

Location. Physical location of the computer to be used with the application.

PART I: The following information is to be provided by the user when establishing or modifying their account. After completing PART 1, the user must first obtain the security manager's signature, and then provide the form to the UAM.

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

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

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

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

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

(6) Job Title/Grade/Rank. The civilian job title, military rank 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, or 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 click in the field to enact a digital signature from their CAC card, 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.

PART II: The information below requires the endorsement of the user's Supervisor/UAM or Government Sponsor.

(13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Can also be used to explain the purpose of the request.

(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 configurations.)

(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.

(20a)Supervisor's Signature. Supervisor must click in the field to enact a digital signature from their CAC card. 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.

(18) 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. The IAO or Appointee of the office responsible for approving access to the system being requested must click in the field to enact a digital signature from their CAC card.

(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.

(26) Name. Repeat data entry of requesting user's name.

(27) Optional Information. This item is used to clarify TC-AIMS II requests for Initiation and Modification. For Initiation, only the ADD Access area is used. For Modification, the ADD Access and/or REMOVE access areas can be used. The information in these areas aid the PD TIS CSC in account creation and maintenance. In both areas, field definitions are:

Unit Name: the user's assigned UIC name

Assigned UIC: the user's Assigned Unit ID in the CoC

Responsible UIC: the most senior parent UIC in the CoC for the user is used as the Responsible Unit ID

Preference UICs: subordinate units to the user's Responsible UIC

Preference Jobs: define the level of access or capability granted to the user within different categories of the TC-AIMS II applications

Primary Job Role(s): user's functional job responsibility(s).

C. PART III: Security Manager's Certification of Clearance.

(28) Type of Investigation. The user's last background investigation (e.g., 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.

PART IV: This information is site specific, and can be customized by the DoD, functional activity, or customer (e.g. the Customer Service Center, IT OPS, etc.) with approval of the DoD. This information will specifically identify the access required by the user.

DISPOSITION OF DD FORM 2875:

Request Initiation: The Request Detail and Part I of this form must be filled out, and digitally signed, by the user requesting access. When the user (requestor) attempts to digitally sign the form in Part I, the user will be forced to save the form, and **must** rename the form using the following format "*SAAR-UserName.PDF*".

Transmission: ***The form must be forwarded by e-mail***, to each entity or person, that's required to fill out and digitally sign the form. Typically the form would pass from the requesting user to the Security Manager, then from the Security Manager to the Unit Account Manager (UAM), then from the UAM to PD TIS Customer Service (the Support and Operations Center). c4isr.support@us.army.mil <mailto:c4isr.support@us.army.mil> is the URL for PD TIS Customer Service (the Support and Operations Center).

Filing: Original SAAR, with digital signatures in Parts I, II, and III, must be maintained on file for one year after termination of a user's account.