DD FORM 2875 - SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

"RED" Fields are Mandatory

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

SYSTEM NAME *(Application Platforms)*
☐ TC-AIMS II

LOCATION

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 and/or functional level access.)*
☐ *I have completed annual Information Awareness training.* COMPLETION DATE *(YYYYMMDD)*

11. USER DIGITAL SIGNATURE *(or UAM digital signature for ACTIVATION, DELETION or DEACTIVATION requests)* 12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY UAM (OR USER'S SUPERVISOR).
(If user is a contractor - please provide Company Name, Contract Number and Date of Contract Expiration in Block 15.)

13. JUSTIFICATION FOR ACCESS (**FOR UAM OR SUPERVISOR USE ONLY - REQUIRED FOR ALL INITIAL AND MODIFICATION REQUESTS**)

14 VERIFICATION OF NEED TO KNOW	15. ACCESS EXPIRATION DATE *(Include Contractor Name and Contract Number)*
I certify that this user requires access as requested. ☐	Leave blank for military personnel

16. ACCESS REQUEST INFORMATION

ADD - ACCESS

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

PreferenceUICs:

Preference Jobs:

Choosing a Preference Job that begins with double asterisks (**), will require additional approval from AMIS.

View Job Profile Details

Primary Job Role(s):

DODAAC
(Required for Jobs: 40, 45, 46 47, 51, 53, 54)

17. ACCESS REQUEST INFORMATION		
PART II - ENDORSEMENT OF ACCESS BY USER'S SUPERVISOR OR UAM (CONT.)		
18. SUPERVISOR OR UAM NAME	19. SUPERVISOR OR UAM E-MAIL ADDRESS	20. PHONE NUMBER
21. SUPERVISOR OR UAM ORG/DEPT	22. SUPERVISOR OR UAM DIGITAL SIGNATURE	23. DATE *(YYYYMMDD)*

PART III - SECURITY MANAGER VALIDATION OF BACKGROUND INVESTIGATION AND CLEARANCE INFORMATION			
24. TYPE OF INVESTIGATION		25. DATE OF INVESTIGATION *(YYYYMMDD)*	
26. CLEARANCE LEVEL		27. IT LEVEL DESIGNATION	
28. VERIFIED BY *(Print name)*	29. SECURITY MANAGER PHONE NUMBER	30. SECURITY MANAGER DIGITAL SIGNATURE	31. DATE *(YYYYMMDD)*

PART IV - COMPLETION OF REQUEST REVIEW AND ACCOUNT CREATION		
32. INFORMATION OWNER DIGITAL SIGNATURE (AMIS)	33. PHONE NUMBER	34. DATE *(YYYYMMDD)*
35. ACCOUNT PROCESSOR DIGITAL SIGNATURE (ASD)	36. PHONE NUMBER	37. DATE *(YYYYMMDD)*

AMIS - DD FORM 2875 INSTRUCTIONS

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

REQUEST DETAIL:

Type of Request. Account request selection. Choose either:
- •Initial - New account creation (User).
- •Modification - To make changes to an existing account (User or UAM).
- •Deletion - Removing an account from the system (UAM).
- •Deactivate - Temporary deactivate an account (Call ASD).
- •Activate - Reactivate a previously deactivated account (Call ASD).

User ID. Unique, system generated user identifier.

Date of Request. Date request was initiated.

System Name. Application platform to be initiated.

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

PART I: The following information is to be provided by the user when establishing or modifying their account. After completing PART I, the user should 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 commercial or the Defense Switching Network (DSN) phone number of the user.

(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 they've completed Information Awareness Training date.

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

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

PART II: The information below requires the endorsement of the user's UAM or government sponsor. After completing PART II, the UAM should forward the Form to the Security Manager.

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

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

(16) Access Request Information. Used to add access for new accounts or to modify existing accounts.
- •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. You must have approval from AMIS before choosing Preference Jobs that begin with double asterisks (**). Use the Job Details Lookup button to view each Job definition in detail.
- •DODDAC: DODDAC entry required for Job IDs 40, 53 and 54.
- •Primary Job Role(s): User's functional job responsibilities.

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

(18) Supervisor or UAM Name. Name of the user's UAM or Supervisor.

(19) Supervisor or UAM E-mail Address. E-mail address of the user's UAM or Supervisor.

(20) Telephone Number. The commercial or the Defense Switching Network (DSN) phone number of the user's UAM or Supervisor.

(21) Supervisor or UAM Org/Dept. Organization or Department of the UAM or Supervisor.

(22) Supervisor or UAM Digital Signature. The UAM or Supervisor must click in the field to enact a digital signature from their CAC card.

(23) Date. The date that the UAM or Supervisor signs the form.

PART III: Security Manager's Certification of Clearance. After the Security Manager completes the investigation and signs PART III, the form is forwarded to the AMIS Service Desk (ASD).

(24) Type of Investigation. The user's last background investigation.

(25) Date of Investigation. Date of last investigation.

(26) Clearance Level. The user's current security clearance level.

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

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

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

(30) Security Manager Signature. The Security Manager or their representative indicates that the above clearance and investigation information has been verified.

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

PART IV: Sign-off and completion of request by authorized staffs (request acceptance by the AMIS staff and account creation by the ASD staff).

(32) Information Owner Digital Signature (AMIS). AMIS representative must click in the field to enact a digital signature from their CAC.

(33) Phone Number. Phone number of AMIS representative.

(34) Date. The date the form was signed by the AMIS representative.

(35) Account Processor Digital Signature (ASD). ASD representative must click in the field to enact a digital signature from their CAC.

(36) Phone Number. Phone number of the ASD representative.

(37) Date. The date that the form was signed by the ASD representative.

DD FORM 2875 – DISPOSITION AND FAQs

***Request Initiation*:** For Initial requests, REQUEST DETAIL and PART I of this form is filled out and digitally signed by the user requesting access. For Activation, Deactivation and Delete requests, the UAM will fill out portions of REQUEST DETAIL and PART I of this form. Modification requests can be initiated by the user, or by the UAM. Either the user or UAM fills out portions of REQUEST DETAIL and PART I on this form. However, only the UAM can make the necessary modifications to PART II. After each user digitally signs of this form, they will be forced to save the form using a different name (e.g. Form2875-*UserName*.pdf).

***Form Routing Paths*:** After initiating a request, the DD Form 2875 should be forwarded by e-mailed, to the next entity required to digitally sign and/or process the form. For INITIAL requests, the form typically passes from the requesting user to the User Account Manager (UAM), then from the UAM to Security Management (JPAS), from JPAS back to the UAM, then from the UAM to the AMIS Service Desk (ASD). For other requests (e.g. Activation, Deactivation and Delete), forms are typically e-mailed directly from the requestor (UAM) to the ASD. **NOTE: All e-mails containing PII must be encrypted.**

The AMIS Service Desk (ASD) telephone number and e-mail address are:

1 (800) 877-7925

usarmy.belvoir.peo-eis.mbx.amis-service-desk@mail.mil

***Form Retention and Dormant Account Policies*:** All digitally signed DD Form 2875s received by ASD are kept on file for one year following termination of the user's account. The Dormant Account Policy states that:
- If a user's account has been inactive for 90 days, an email notice will be sent to the user instructing them to log into their account, or the account will be deactivated at 120 days.
- At 120 days, if still no activity, the account will be deactivated.
- Accounts not reactivated after 180 days, will be deleted. The user must then submit a new DD Form 2875, to have a new account established.