

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DOD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.

TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DELETION	DATE
--	------

PART I (To be completed by User)

1. NAME (LAST, First, MI)	2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. ACCOUNT CODE N/A
6. JOB TITLE/FUNCTION	7. GRADE/RANK	8. PHONE (DSN)
9. EMAIL ADDRESS		

STATEMENT OF ACCOUNTABILITY

I understand my obligation to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized access.

USER SIGNATURE	DATE
----------------	------

PART II (To be completed by User's Security Manager)

10. CLEARANCE LEVEL	11. TYPE OF INVESTIGATION	12. DATE OF INVESTIGATION
13. VERIFIED BY (Signature)	14. PHONE NUMBER	15. DATE

PART III (To be completed by User's Supervisor)

16. ACCESS REQUIRED (Circle Service) - USA USMC USAF USN Other	17. ACCESS TO CLASSIFIED REQUIRED? <input checked="" type="checkbox"/> NO <input type="checkbox"/> YES	18. TYPE OF USER <input checked="" type="checkbox"/> FUNCTIONAL <input type="checkbox"/> SYSTEM	<input type="checkbox"/> SECURITY ADMINISTRATOR <input type="checkbox"/> APPLICATION DEVELOPER <input checked="" type="checkbox"/> OTHER (Specify)
--	---	--	--

19. JUSTIFICATION FOR ACCESS To access TATRC AAMTI system.
--

VERIFICATION OF NEED TO KNOW

I certify that this user requires access as requested in the performance of his/her job function.

20. SIGNATURE OF SUPERVISOR	21. ORG./DEPT.	22. PHONE NUMBER	23. DATE
24. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR	25. ORG./DEPT.	26. PHONE NUMBER	27. DATE

PART IV (To be completed by AIS Security Staff adding user)

28. USERID (Mainframe) N/A	29. USERID (Mid-Tier) N/A	30. USERID (NETWORK/SYSTEM)
31. SIGNATURE	32. PHONE NUMBER	33. DATE

INSTRUCTIONS FOR FORM 41

A. PART I: *(The following information is completed by the user when establishing their USERID.)*

TYPE OF REQUEST: **X INITIAL**

DATE: Today's date

(1) NAME: Your name (Last, First, Middle Initial)

(2) SOCIAL SECURITY NUMBER: Your Social Security Number (Box 2 is not required, if you hold a valid Security Clearance and Part II is completed in its entirety.)

(3) ORGANIZATION: Your organization or activity. (i.e., USAMRMC-TATRC)

(4) OFFICE SYMBOL/DEPARTMENT: Your office code or department name (i.e., MCMR-TT)

(5) ACCOUNT CODE: For those with no TATRC Site affiliation, insert "N/A."

(6) JOB TITLE/FUNCTION: Selecting ONLY ONE, insert the position description that best describes your job.

(7) GRADE/RANK: Your civilian pay grade, military rank or CONT if contractor.

(8) PHONE (DSN): Your Defense Switching Network (DSN) phone number. If DSN is unavailable, indicate commercial phone number.

(9) E-MAIL ADDRESS: Your e-mail address. This cannot be a group or organizational e-mail address.

USER'S SIGNATURE: You must sign the SAAR form with the understanding that you are responsible and accountable for your password and access to the system(s).

B. PART II: *(The following information is to be provided by the User's Security Manager.)*

Note: Users who have been asked to apply for USERID and who DO NOT have a valid security clearance should write N/A in Box 10 and enter their Social Security Number in Part I, Box 2. Users who DO have a security clearance must have Part II executed by their organization's Security Manager.

(10) CLEARANCE LEVEL: The user's current security clearance level and ADP Level (i.e., Secret, Top Secret, ADP I, ADP II, etc.) Note: You may need to check with your LAN S/A for your ADP level.

(11) TYPE OF INVESTIGATION: The user's last type of background investigation. (i.e., NAC, NACI, or SSBI)

(12) DATE OF INVESTIGATION: The date of the last background investigation.

(13) SIGNATURE: The Security Manager or his/her representative's signature indicates that the above clearance and investigation information has been verified.

(14) PHONE: The Security Manager's phone number.

(15) DATE: The date that the form was signed by the Security Manager or his/her representative.

C. PART III: *(The following information is to be provided by the User's Supervisor or Manager.)*

(16) ACCESS REQUIRED (Location):

(17) ACCESS TO CLASSIFIED REQUIRED? **No**

(18) TYPE OF USER: **Functional; X - Other (specify): End User**

(19) JUSTIFICATION FOR ACCESS: **To access System.**

(20) SIGNATURE OF SUPERVISOR: The user's supervisor or COI Manager must sign the SAAR form to certify the user is authorized access to perform his/her job function.

(21) ORG/DEPT.: Supervisor's .

(22) PHONE NUMBER: Supervisor's or Manager's phone number.

(23) DATE: The date the Supervisor or Manager signs the SAAR.

(24) SIGNATURE OF FUNCTIONAL DATA OWNER/OPR: Signature of the functional appointee responsible for approving access to the system being requested.

(25) ORG./DEPT.: Functional appointee's organization and department.

(26) PHONE NUMBER: Functional appointee's phone number.

(27) DATE: The date the Functional appointee signs the SAAR.

D. PART IV: *(The following information is provided by TATRC AIS Security Staff who adds the user to the system.)*

(28) USERID (Mainframe): **N/A**

(29) USERID (Mid-Tier): **N/A**

(30) USERID (Network/System): Network/System ID assigned to the user.

(31) SIGNATURE: Signature of the Information Systems Security Officer (ISSO) or his/her representative.

(32) PHONE NUMBER (DSN): The ISSO's DSN phone number.

(33) DATE: The date the ISSO signs the SAAR.

FORM 41 FAQ

1. IS THIS FORM BEING USED TO VALIDATE A SITE OR AN INDIVIDUAL?

AN INDIVIDUAL.

2. SSN REQUIRED?

IT'S ONLY REQUIRED IF YOU DO NOT HOLD A VALID SECURITY CLEARANCE. IF YOU DO HOLD A SECURITY CLEARANCE, SKIP BOX 2, AND VERIFY THAT PART II IS COMPLETED IN ITS ENTIRETY.

3. HOW ABOUT USERS WITH MULTIPLE SITE IDS?

USE THE SITE ID WHERE YOU DO MOST OF YOUR WORK.

4. CAN I LIST A GROUP OR ORGANIZATION EMAIL ADDRESS?

NO.

6. HOW WILL I KNOW MY FORM HAS BEEN SUCCESSFULLY PROCESSED?

TATRC WILL SEND A VALIDATION ACKNOWLEDGEMENT VIA EMAIL.

7. ONCE TATRC RECEIVES A COMPLETED FORM 41, HOW LONG DOES IT TAKE TO VALIDATE A USER REQUEST FOR AN ID?

APPROXIMATELY 2-4 BUSINESS DAYS.

8. HOW LONG WILL THIS FORM BE VALID?

FOR AS LONG AS YOU ARE A USER.

9. HOW LONG WILL PASSWORDS BE VALID?

90 DAYS.

12. HOW DO I SEND THE FORM 41 BACK TO THE OPERATIONS CENTER?

BY FAX to 301-619-5067 or encrypted email to willie.wright@amedd.army.mil