

Office of the Administrative Assistant to the Secretary of the Army,
United States Information Technology Agency (AAIT-DC)

LOGONID REQUEST FORM

PLEASE PRINT and COMPLETE ALL SECTIONS. Improper submissions will be returned.

PART A USER INFORMATION

- 1. FULL NAME (LAST) (FIRST) (MI) 2. SSN
3. RANK/GRADE/ CONTRACTOR 4A. ORGANIZATION/UNIT 4B. OFFICE SYMBOL
5. OFFICE PHONE: (COMMERCIAL) () DSN:
6. REQUESTOR'S ORGANIZATION MAILING ADDRESS (NO ACRONYMS PLEASE) ATTN: (STREET ADDRESS, P.O. BOX) (CITY) (STATE) (ZIP)
7. LIST ANY PREVIOUS AAIT-DC (NISA) LOGONIDS ISSUED:
8. USER EMAIL ADDRESS

PART B PLEDGE TO UPHOLD SECURITY STANDARDS

I certify that I have read, understand, and will comply with the security policies and procedures described in the "User Responsibilities" section of this form. I understand that any violations of these procedures by me, any unauthorized use of Government resources, or withholding knowledge of any suspected violation may result in suspension/termination of my user privileges on the AAIT-DC system and submission of a report to my supervisor.

SIGNATURE DATE

PART C SECURITY VERIFICATION

All users must have at least a favorable NAC completed and verified by your security office in order to access the AAIT-DC system.

1. I certify that (Full Name) holds a valid clearance level of

issued on (DD/MM/YY) by (ISSUING AGENCY)

Type of investigation Date completed (DD/MM/YY)

2. I have reviewed this request and certify that the applicant has a need for access to the AAIT-DC system and has been briefed on terminal area security.

CIRCLE THE SYSTEM(S) TO BE ACCESSED: ATRRS MODS PAM OTHER

Security Manager (TYPE / PRINT NAME) (SIGNATURE) (PHONE#)

CONTRACTOR INFORMATION

- 1. COMPANY NAME 2. CONTRACT#
3. EFFECTIVE DATE 4. EXPIRATION DATE
5. COR/COTR (TYPED NAME) (SIGNATURE) (PHONE)

MEDPROS USERS (REQUIRED)

(MARK ONE) ___Active Army ___National Guard ___Reserve ___Mobilized Reservist/Guard ___DA Civilian ___Contractor

Commander (Active Army), State (Guard), RSC/O&F/Training Command (Reserve) Approval Authority.

A commander or SRP OIC is the approval authority for DA Civilians and Contractors.

 (RANK) (POS TITLE) (PRINT NAME) (SIGNATURE) (PHONE #)

(Guard and Reserve only) Allow user to update physicals in MEDPROS **(CIRCLE ONE) APPROVED DISAPPROVED**
 Approve the above named person to receive MEDPROS "Write Access" as the commander's representative and further certify that the applicant has met the minimum security requirement NAC favorably completed and has been briefed by the Information Systems Security Office (ISSO). He/She understands the data contained within the MODS/MEDPROS Mainframe and Web is for Official Use Only and is not intended and cannot be used for any other purpose.

PAM USERS

JUSTIFICATION FOR ACCESS TO THE PAM SYSTEM: _____

ATRRS Connection Survey

Please complete this form carefully. If you are not sure of an answer get assistance from someone in your office. **Erroneous information could result in not getting the software that may be required to access the ATRRS system.** Please forward this survey along with your AAIT-DC LOGON-ID request form to the address at the bottom of the AAIT-DC Form 9-R. **PLEASE TYPE OR PRINT.**

PART A - ORGANIZATION INFORMATION

1. FULL NAME _____ 2. SSN _____
 (LAST) (FIRST) (MI)
 3. RANK/GRADE/TITLE _____ 4A. ORGANIZATION ACRONYM _____
 4B. OFFICE SYMBOL ATTN: _____
 4C. ADDRESS 1 _____
 4D. ADDRESS 2 _____
 4E. CITY _____ 4F. STATE _____ 4G. ZIP _____
 5. COMM. OFFICE PHONE: (_____) _____ DSN: _____
 6. FAX OFFICE PHONE: (_____) _____ DSN: _____

PART B - SYSTEM INFORMATION

Is your ATRRS site Active Army _____ Army Reserve _____ Army National Guard _____?
 If none of the above, please indicate _____
 Does the computer you will be using already have ATRRS connectivity? Yes _____ No _____
 Is your computer connected to a local area network (LAN)? Yes _____ No _____
 Do you have Internet access? Yes _____ How _____ No _____

PART C - TSACS MODEM CONDUCTIVITY

Army National Guard and Army Reserve Personnel who require modem connectivity can use the Terminal Server Access Controller System (TSACS).

To allow access to the NIPERNET. Through the NIPERNET, authorized users can connect to the Pentagon mainframe computer, and the ATRRS Website www.atrrs.army.mil via modem to access the Army Training Requirements and Resource System (ATRRS).

NOTE: Active Army Personnel must contact their Local Director of Information Management (DOIM) for a TSACS Account. If you need a TSACS Account for ATRRS connectivity, please indicate. Yes _____ No _____

INSTRUCTIONS

PART A

- #4. Use official organization and office symbol. Contractors must enter COTRs Office Symbol.
- #6. Requestor Organization's complete address, no acronyms please. Include room and building numbers required
- #8 Prefer AKO email address.

PART B ALL APPLICANTS MUST READ AND SIGN.

PART C You may not verify your own clearance.

CONTRACTORS are required to submit a Visit Authorization Request (**VAR**) signed by their Corporate Security Officer. The VAR must be on company letterhead, and include the persons name, date and place of birth, SSN, citizenship, investigation information and clearance information; any questions please refer to Army Regulation 25-2.

PAGE 2 All sections that are applicable to the user must be completed.

ISSO/COR must fax this form to:

**MODS Help Desk:
Attn User Access:
Fax (703) 681-4983 Comm: (703) 681-4976**

**If a mailing address is needed
please send a request to:
mods-help@asmr.com**

PRIVACY ACT STATEMENT

AUTHORITY: EXECUTIVE ORDER 10450.

Personal information on this form is used to determine the individual's eligibility for access to AAIT-DC computer resources.

Provided information is used to ensure that only authorized personnel access the computer resources.

DISCLOSURE OF INFORMATION ON THIS FORM IS VOLUNTARY. HOWEVER, IF THE INFORMATION IS NOT PROVIDED, SYSTEM ACCESS WILL BE DENIED.

USER RESPONSIBILITIES

- A.** Fill out the AAIT-DC LOGON-ID Request Form (AAIT-DC Form 9R) completely. Incomplete forms will be returned.
- B.** Follow proper LOGON and LOGOFF procedures.
- C. Change PASSWORDS at least once within a 90-day period.** The PASSWORDS are computer generated, but the process **must be initiated by the user.**
- D.** Ensure each remote terminal is active only when an authorized terminal operator is present and using the equipment. Any violation of this procedure is a breach of security. Prior to leaving the terminal, each user must properly LOGOFF to ensure access cannot be gained without initiating proper LOGON procedures.
- E.** Adhere to security requirements for all remote terminals, individual passwords, and data transmitted to and from the AAIT-DC ADP System(s).
- F.** Handle all information from the AAIT-DC database containing personal/privacy act information as sensitive data and comply with provisions of the Privacy Act and other published security procedures.
- G.** Prevent unauthorized disclosure or transfer of systems entry features from one user to another. **DO NOT SHARE TERMINAL SESSIONS or PASSWORDS!** Violations of this will result in suspension of access. Access will be restored upon receipt of a letter from the security manager stating the violation, the name(s) of individual(s) involved, and their SSN's.
- H.** Do not transmit and/or extract classified data via unclassified remote terminals.
- I.** Report suspected security violations to your supervisor and Security Manager.
- J.** Do not attach privately owned equipment to the AAIT-DC computers.
- K.** If you have any questions about this form please call the Access Management Help Desk at 703 693-3625 or DSN 223-3625.

Contracting Company's entire Letterhead

(not military facility)
(form Must be completely typed)

To: ASM Research, Inc.
ATTN: MODS Support Team

3025 Hamaker Court, Suite 100
Fairfax, VA 22031
Fax # 703.681.4983 DSN 761.4983

**(This form is only required for Contractor's)
VISITOR ACCESS REQUEST (VAR)**

Questions 1 – 5 are REQUIRED for all access requests.

1) Name and Address of Agency to be visited: MODS, ASM Research, Inc.

2) Name of Visitor:
Date of Birth:
Place of Birth:

Citizenship:

SSN:

3) Job Title of Visitor:

4) Period of Visit (To and From Dates not to exceed one year):

5) Purpose and Justification for visit (Job description and modules requested. IE: MODS/MEDPROS, PERSONNEL Web, ...):

6) Type of Investigation and Date:

Investigation Completed/Initiated By:

COGNIZANT SECURITY OFFICE:
(Fill in if Security Clearance info is filled in)

Initiating Security Office Address:

I certify that the security clearance granted this facility and the security clearance granted the person listed above are correct as stated.

Name of Facility Security Officer (Sign if Clearance information is filled in)

NEED TO KNOW FOR THIS VISIT IS CERTIFIED AS VALID

Visitor's Project Manager/ Project/ Organization / Phone Number **(Required)**