UPROD TCPT users are required to have a SAAR and Cyber Awareness Training Certificate on file with the MLS2 project office for account access. These instructions are for requesting an account in a NIPR environment. If you are looking for an unclassified account in a SIPR environment, please go to https://mls2support.atlassian.net/servicedesk/customer/portal/2/article/1678016513. A downloadable SAAR, instructions on completing the SAAR, and instruction on submitting the documents are below.

Instructions

1. Header and Part I: Completed by user

   a.

   b. All blocks must be complete.
   c. Type of request: Must be Initial, Modification, or Deactivate
      i. INITIAL: Should be selected if:
         1. User has never been issued a System/Application account before
         2. User's prior account was deleted

3. User is changing from Civilian/Military to Contractor or vice versa (see exception under "Modification")

    ii.   MODIFICATION: Should be selected if:

1. User at one time changed from Military to Contractor and now is transitioning to Civilian (exception to the last bullet under "Initial")
2. User moved to different Command or Base
3. User needs to reactivate an already existing account
4. User is requesting a name change
5. User is renewing their CAC or Changing contract numbers
6. User has a new job title
7. User is changing from Military to Civilian

    iii.   DEACTIVATE

1. Select when requesting the user's account to be deactivated. This is usually requested when a user is leaving the Command or contract supporting the Command. It is recommended to submit the SAAR 5 to 10 days prior to the user leaving. *User's Government Sponsor/Supervisor is responsible for ensuring the account deactivation request is submitted to the Help Desk.

d. System name: TCPT

e. LOCATION *(Physical Location of System)* MUST be **HCS Kansas City** no matter where you are located.

f. Block 1: Your name.

g. Block 2: Your government agency.

h. Block 3: Your units name.

i. Block 4: A number you can be reached at.

j. block 5: The email address issued to you by a government agency.

k. Block 6: Your Job Title and Rank

l. Block 7: is your units mailing address.

m. Blocks 8 and 9 are specific to you and must be checked

n. The date in block 10 must match the date on the cyber awareness certificate you provide.

    i.   This is the current list of accepted certificates.

1. Option 1 - Cyber Awareness & PII Combined Certification

    a. **CYBERM0000** USMC Cyber Awareness Training (Marine Net) (active and reserve military only)

    b. **CYBERC** Civilian Cyber Awareness Training (Marine Net) (contract and civilian employees)

        c. **CYBERINTEL** Intelligence Community Cyber Awareness Training Curriculum

        d. **ANNUALTRFY**Annual Training Curriculum Fiscal Year (MarineNet)

2. Option 2 - Cyber Awareness + PII individual courses

        a. **DODCAC1000** DOD Cyber Awareness Challenge + **DONPII010A** Department of the Navy Annual Privacy Training (Marine Net)

        b. **DOD-IAA-V17.0** Cyber Awareness Challenge V5 + **DON-PRIV-2.0** Department of the Navy Annual Privacy Training (TWMS)

        c. Cyber Awareness Challenge + Identifying and Safeguarding Personally Identifiable Information (PII) (DISA)

        d. **INTELCAC** Cyber Awareness Challenge (Intel Community) + **DONPII010A** Department of the Navy Annual Privacy Training (Marine Net)

o. Your digital signature is required in block 11. Ensure the date in block 12 is the same date you digitally sign block 11.

2. Part II: Completed by supervisor

a.

13. JUSTIFICATION FOR ACCESS
Site: (I MEF, II MEF, III MEF, MFR, etc)
Application role requested: (General user, Unit Chief, Unit Supervisor, etc)
Environment: NIPR Production
Risk: MARADMIN 229/22
Access needed for daily duties

14. TYPE OF ACCESS REQUESTED
☐ AUTHORIZED   ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)* _____
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)*	
☐ I certify that this user requires access as requested.		
17. SUPERVISOR'S NAME *(Print Name)*	**17a. SUPERVISOR'S EMAIL ADDRESS**	**17b. PHONE NUMBER**
17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT	**17d. SUPERVISOR SIGNATURE**	**17e. DATE** *(YYYYMMDD)*
18. INFORMATION OWNER/OPR PHONE NUMBER	**18a. INFORMATION OWNER/OPR SIGNATURE**	**18b. DATE** *(YYYYMMDD)*
19. ISSO ORGANIZATION/DEPARTMENT	**19b. ISSO OR APPOINTEE SIGNATURE**	**19c. DATE** *(YYYYMMDD)*
19a. PHONE NUMBER		

DD FORM 2875, MAY 2022   UNCLASSIFIED ▾   Page 1 of 3
PREVIOUS EDITION IS OBSOLETE.

b. Block 13- Justification must match the system listed in the system name block.
  i. A concise statement for why access is required along with the following information:
    1. Site: Your location
    2. Application role requested
    3. Environment is NIPR Production
    4. Any additional detail to specify access requirements
      a. Example
        i. Example for STRATIS SAAR

          Site: BIC

          Role: ADM

          Permission Group: Interface User

          Risk: Annually Validation
      ii. Example for CLC2S

          Site: (I MEF, II MEF, III MEF, MFR, etc)

Application role requested: (Clerk, Principal Staff, Rations Coordinator, Corpsman, or Unit Supervisor)

Environment: NIPR Production

Risk: MARADMIN 229/22

    iii.   Example for TCPT

Site: (I MEF, II MEF, III MEF, MFR, etc)

Application role requested: (General user, Unit Chief, Unit Supervisor, etc)

Environment: NIPR Production

Risk: MARADMIN 229/22

    c.   Block 14- Authorized must be checked
    d.   Block 15- Unclassified must be checked
    e.   Block 16- must be checked
    f.   Block 16a- is a requirement for all contractors. This block is not a requirement for military and DOD personnel.
    g.   Blocks 17 through 17e must be filled in
    h.   Blocks 18 through 19c must be blank. After you submit your SAAR, the helpdesk will send your SAAR to MARCORSYSCOM for approval. They will complete this portion.

3.   Part III: Completed by security manager.

    a.

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION				
22. TYPE OF INVESTIGATION			22a. INVESTIGATION DATE *(YYYYMMDD)*	
22b. CONTINUOUS EVALUATION (CE) ENROLLMENT DATE *(YYYYMMDD)*		22c. ACCESS LEVEL		
23. VERIFIED BY *(Printed Name)*	24. PHONE NUMBER	25. SECURITY MANAGER SIGNATURE		26. VERIFICATION DATE *(YYYYMMDD)*

    b.   Ensure blocks 22 through 26 are filled.

Before you submit your documents, please name them according to this naming convention

1. Doe_MIL_Jane_A_CyberAwareness_YYYYMMDD
2. Doe_MIL_Jane_A_PII_YYYYMMDD
3. Doe_MIL_John_A_SYSTEM_Authorized_SAAR_YYYYMMDD

<u>Helpful tip</u>

- You can edit some SAARs by clicking your digital signature, remove it, and it will unlock a portion of the SAAR. The users digital signature locks Part I, the supervisors digital signature locks Part II, and the security managers signature locks Part III.

To submit your documents for account approval you can;

Post them here
https://mls2support.atlassian.net/servicedesk/customer/portal/2/group/2/create/50

or

Email them to support@mls2support.com

If you have any questions please call (888) 529-6516.

Highlight important information in a panel like this one. To edit this panel's color or style, select one of the options in the menu below.