Creating an Auto SAAR Account Request

Log onto Auto SAAR portal using the following link below

https://autosaar.usmc.mil

Click Accept
Click on Marine Corps University then Submit
Select the type of request.
Select your role.
The following line is for your EDIPI number that is located on the back of your CAC.
Finally you will add your Justification for Access and click continue.
Electronic Signature Confirmation:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) which includes any device attached to this information system that is provided for U.S. Government authorized use only.
- You consent to the following conditions:
  - The U.S. Government routine intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - Communications using or data stored on this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used by any U.S. Government authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests not for your personal benefit or privacy.
  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
    - The user consents to interception/interception or seizure of all communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/interception or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on matters prior to using an information system. If the user intends to rely on the protections of a privilege or confidentiality:
      - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy.
      - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DOD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
      - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take reasonable measures to protect the content of captured/seeded privileged communications and data to ensure they are appropriately protected.
    - In cases where the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants, the U.S. Government may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise authorized use or disclosure of such information.
    - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to inform the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.
Click the box stating that you have read and agree with the terms and conditions. Click E-Sign.
You will now be returned to the home screen where you can see the status of your requests.

You will now receive email notifications as your SAAR request moves forward.