
SECURITY

REQUEST FOR ACCESS, PLAN OF ACTION

1. Purpose. To provide the Information Systems Security Manager (ISSM), Information System Security Officers (ISSOs), and individuals requesting ATAAPS access with guidance regarding access to system resources and use of DISA Form 41, System Authorization Access Request (SAAR).
2. Background. This plan of action is designed to ensure compliance with the Information Systems Security Program.
3. Scope. This SOP applies to all new ATAAPS users.
4. New User Process.
 - a. Supervisor will request access to ATAAPS via a DISA Form 41, 30 days prior to production.
 - b. Supervisor will obtain employees signature and forward form to the remote Security Manager (SM).
 - c. The remote SM will verify security clearance and/or investigation, annotate the form and forward to the appointed remote ATAAPS POC. Upon receiving request the remote ATAAPS POC confirms that clearance and/or investigation have been verified. The remote ATAAPS POC will then forward form to Regional Support Activity Chambersburg (RSA Chambersburg) ISSO.
 - d. RSA ISSO will create the user-id using the DISA LAN account provided in Block 29 of the DISA Form 41.
 - e. RSA ISSO will provide the remote ATAAPS POC with the password.
5. Existing User Process.
 - a. If an existing account becomes locked or a user forgets their password, the user will contact the remote ATAAPS POC who will in turn notify RSA ISSO via e-mail. RSA ISSO will reset the account and notify the remote ATAAPS POC upon completion of reset via e-mail.
 - b. It is requested that 2, possibly 3 remote ATAAPS POC names be provided to RSA ISSO for the purpose of new accounts and password reset requests.
6. It is the supervisors responsibility to ensure that if deletion of access is required, that a SAAR be submitted to security reflecting removal of account.
7. New and deletion examples of the DISA Form 41 are included.

RONALD E. WISE
Director
Regional Support Activity Chambersburg