SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)										
PRIVACY ACT STATEMENT AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.										
TYPE OF REQUEST		DATE (YYYYMMDD)								
SYSTEM NAME (<i>Platform or Applications</i>) CS AIX server account, UNIX OOB access account	LOCAT	TION (Physical Location of System) DISA SATX, DISA OKC								
PART I (To be completed by Requestor)										
1. NAME (Last, First, Middle Initial)		2. ORGANIZATION								
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commerce	cial)	9						
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/	RANK							
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP		9. DESIGNATION MILITARY	CIVILIAN OR					
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) I have completed Annual Information Awareness Training. DATE (YYYYMMDD)										
11. USER SIGNATURE				12. DATE (YYYY)	MMDD)					
contractor - provide company name, contract number, and d										
14. TYPE OF ACCESS REQUIRED:										
15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED (Specify category)										
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested.	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)									
17. SUPERVISOR'S NAME (Print Name)	18. SUPI	ERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)							
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS 20b. PHONE NUMBER									
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER			21b. DATE (YYYYMMDD)						
22. SIGNATURE OF IAO OR APPOINTEE	23. ORG	ANIZATION/DEPARTMENT	24. PH0	DNE NUMBER	25. DATE (YYYYMMDD)					

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional information)

1.) User Name (Last, First, Middle In.):

2.) Date of Birth (MM/DD/YYYY):

3.) EDIPN (10 digit number on the back of your CAC):

4.) DSA # (Required for contractors):

5.) PIN:

OOB Access to SATX/OKC with UNIX profile.

Server account creation on the following AIX servers:

Production SCE: cship-name usatix8v Production MCAT: cship-name usatix8z, set rlogin=false and login=true

ProdTest SCE:cship-name utinip1q ProdTest MCAT: cship-name utinip1s, set rlogin=false and login=true

Set Primary Group set to "sce"

SATX SA: Once OS accounts are created on the AIX Servers please DO NOT notify the user. Instead please notify the SDD Access Office and SDD DP Ops personnel that the ID has been created.

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION									
28. TYPE OF INVESTIGATION 28b. CLEARANCE LEVEL		28a. DATE OF INVESTIGATION (YYYYMMDD)							
		28c. IT LEVEL DESIGNATION							
29. VERIFIED BY (Print name)		30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE			32. DATE (YYYYMMDD)			
PART IV - COMPLETIO	N BY AUTHORIZED	STAFF PREPARING ACCO	UNT INF	ORMATION					
TITLE:	SYSTEM			ACCOUNT CODE					
	DOMAIN								
	SERVER APPLICATION								
	DIRECTORIES								
	FILES								
	DATASETS								
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)			DATE (YYY	YMMDD)				
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)			DATE (YYYYMMDD)					
				•		1			

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(5)Official E-mail Address. The user's official e-mail address.

(6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(7) Official Mailing Address. The user's official mailing address.

(8) Citizenship (US, Foreign National, or Other).

(9) Designation of Person (Military, Civilian, Contractor).

(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

 $(20) \;$ Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.