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 Social Security Numbers 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 ☐ INITIAL ☐ MODIFICATION ☐ DELETION ☐ USER ID _____	DATE
SYSTEM NAME *(Platform or Applications)*	LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*		2. SOCIAL SECURITY NUMBER
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. PHONE *(DSN or Commercial)*
6. OFFICIAL E-MAIL ADDRESS	7. JOB TITLE AND GRADE/RANK	
8. OFFICIAL MAILING ADDRESS	9. CITIZENSHIP	10. DESIGNATION OF PERSON

USER AGREEMENT *(Complete Block 29 or 30 as appropriate)*

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DISA/DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ I have completed Annual Information Awareness Training. DATE _____

11. USER SIGNATURE	12. DATE

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED ☐ PRIVILEGED LEVEL OF CERTIFICATION CLEARANCE _____

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

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	16a. EXPIRATION DATE FOR ACCESS *(Specify date if less than 1 year)*

17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE
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

22. SIGNATURE OF IAO	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE

26. SYSTEM ADMINISTRATOR:
I have completed my Annual Requirement for Information Assurance awareness.
☐ YES ☐ NO DATE _____

27. OPTIONAL INFORMATION

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. CLEARANCE LEVEL	
28b. IT LEVEL DESIGNATION	28c. DATE	28d. TYPE OF DESIGNATION	
29. VERIFIED BY *(Print name)*		30. SIGNATURE	31. DATE

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED	PROCESSED BY *(Print name and sign)*	DATE
DATE REVALIDATED	REVALIDATED BY *(Print name and sign)*	DATE

INSTRUCTIONS

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) Social Security Number. The social security number of user.

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

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

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

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

(7) 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.

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

(9) Citizenship. The user's citizenship status.

(10) Designation of Person.

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 X455 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 GovernmentSsponsor.

(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 X455.

(22) Signature of IAO. Signature of the IAO or sponsoring 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 X455.

(26) System Administrator. Place an "X" in the appropriate box and indicate date Information Assurance requirement was completed.

(27) Optional Information. This item is intended to add site specific information, as required. Contractors include COR name, signature, email address, and/or phone number.

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) Clearance Level. The user's current security clearance level (Secret, Top Secret).

(28b) IT Level Designation. The user's ADP designation (ADP1, ADP3, etc.).

(28c) Date. Date of last investigation.

(28d) Type of Designation. The user's last ADP designation (ADP1, ADP2, etc.).

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

(31) 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.