SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)									
AUTHORITY: PRIVACY ACT STATEMENT PRINCIPAL PURPOSE: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. 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 (YYYYMM	DD)			
		U	SER ID		_				
SYSTEM NAME (Platform	or Applications)			LOCATI	ON (Physical Loca	ation of System)			
PART I (To be completed	hy Requestor)								
1. NAME (Last, First, Mic			2. ORGANIZATION						
3. OFFICE SYMBOL/DEF	PARTMENT		4. PHONE (DSN or Commercial)						
5. OFFICIAL E-MAIL ADDRESS			6. JOB TITLE AND GRADE/RANK						
7. OFFICIAL MAILING AD	DDRESS		8. CITIZENSHIP		9. DESIGNATION OF PERSON				
			US FN		MILITARY	CIVILIAN			
			OTHER		CONTRACT	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 (YYY)	(MMDD)			
	T OF ACCESS BY INFORMATIO any name, contract number, and d			OVERNM	ENT SPONSOR (lf individual is a			
13. JUSTIFICATION FOR	ACCESS								
14. TYPE OF ACCESS RE	EQUIRED:								
AUTHORIZED	PRIVILEGED								
15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED (Specify category)									
16. VERIFICATION OF N	EED TO KNOW	16	a. ACCESS EXPIRATION DA Contract Number, Expiration						
I certify that this user r	equires access as requested.		Contract Number, Expiration	T Date. 0	Se Diock 27 II liee	ueu.)			
17. SUPERVISOR'S NAME (Print Name) 18. SUPERVISOR'S SIGNATURE					19. DATE (YYYYMMDD)				
0. SUPERVISOR'S ORGANIZATION/DEPARTMENT 20a. SUPERVISOR'S E-MAIL ADDRESS				SS	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. PHC	NE NUMBER	25. DATE (YYYYMMDD)			

26. NAME	(Last,	First,	Middle	Initial)
----------	--------	--------	--------	----------

27. OPTIONAL INFORMATION (Additional information)

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION									
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)							
28b. CLEARANCE LEVEL			28c. IT LEVEL DESIGNATION						
29. VERIFIED BY (<i>Print name</i>) 30. SECURITY MANAGER TELEPHONE NUMBER		31. SECURITY MANAGER SIGNATURE 32. DATE (YYYYMMDL							
PART IV - COMPLETIC	PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION								
TITLE:	SYSTEM			ACCOUNT CODE					
	DOMAIN								
	SERVER								
	APPLICATION								
	DIRECTORIES								
	FILES								
	DATASETS								
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)			DATE (YYYYMMDD)					
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)			DATE (YYYYMMDD)					

DD FORM 2875 (BACK), AUG 2009

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.

 $(20) \ \mbox{Supervisor's Organization/Department.} \ \mbox{Supervisor's organization} \ \mbox{and department.}$

(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.

DD 2875 ADDENDUM STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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:

o The U.S. Government routinely 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.

o At any time, the U.S. Government may inspect and seize data stored on this information system.

o 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 for any U.S. Government-authorized purpose.

o 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.

o 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/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Initials _____

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 such 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 all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., 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.

o 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 remind 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 provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Initials _____