SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

OMB No. 0704-0630
OMB approval expires:
20250531

The public reporting burden for this collection of information, 0704-0630, is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450; and Public Law 99-474, the Computer Fraud and Abuse Act

PRINCIPAL PURPOSE(S): 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 USE(S): 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 ☐ DEACTIVATE ☐ USER ID _____

DATE *(YYYYMMDD)*

SYSTEM NAME *(Platform or Applications)*

LOCATION *(Physical Location of System)*

PART I *(To be completed by Requester)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION

3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN or Commercial)*

5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK

7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP	9. DESIGNATION OF PERSON
	☐ US ☐ FN ☐ OTHER	☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

☐ I have completed the Annual Cyber Awareness Training. **DATE** *(YYYYMMDD)*

11. USER SIGNATURE	12. DATE *(YYYYMMDD)*

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 REQUESTED

☐ AUTHORIZED ☐ PRIVILEGED

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

☐ OTHER

16. VERIFICATION OF NEED TO KNOW	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)*
☐ I certify that this user requires access as requested.	

17. SUPERVISOR'S NAME *(Print Name)*	17a. SUPERVISOR'S EMAIL ADDRESS	17b. PHONE NUMBER

17c. SUPERVISOR'S ORGANIZATION/DEPARTMENT	17d. SUPERVISOR SIGNATURE	17e. DATE *(YYYYMMDD)*

18. INFORMATION OWNER/OPR PHONE NUMBER	18a. INFORMATION OWNER/OPR SIGNATURE	18b. DATE *(YYYYMMDD)*

19. ISSO ORGANIZATION/DEPARTMENT	19b. ISSO OR APPOINTEE SIGNATURE	19c. DATE *(YYYYMMDD)*
19a. PHONE NUMBER		

DD FORM 2875, MAY 2022

Page 1 of 3

PREVIOUS EDITION IS OBSOLETE.

20. NAME *(Last, First, Middle Initial)*

21. OPTIONAL INFORMATION

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

22. TYPE OF INVESTIGATION	22a. INVESTIGATION DATE *(YYYYMMDD)*	22b. CONTINUOUS EVALUATION (CE) DEFERRED INVESTIGATION

22c. CONTINUOUS EVALUATION (CE) ENROLLMENT DATE *(YYYYMMDD)*	22d. ACCESS LEVEL

23. VERIFIED BY *(Printed Name)*	24. PHONE NUMBER	25. SECURITY MANAGER SIGNATURE	26. VERIFICATION DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	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, MAY 2022

PREVIOUS EDITION IS OBSOLETE.

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 Cyber 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.

(17a) E-mail Address. Supervisor's e-mail address.

(17b) Phone Number. Supervisor's telephone number.

(17c) Supervisor's Organization/Department. Supervisor's organization and department.

(17d) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(17e) Date. Date the supervisor signs the form.

(18) Phone Number. Functional appointee telephone number.

(18a) Signature of Information Owner/Office of Primary Responsibility (OPR). Signature of the Information Owner or functional appointee of the office responsible for approving access to the system being requested.

(18b) Date. The date the functional appointee signs the DD Form 2875.

(19) Organization/Department. ISSO's organization and department.

(19a) Phone Number. ISSO's telephone number.

(19b) Signature of Information Systems Security Officer (ISSO) or Appointee. Signature of the ISSO or Appointee of the office responsible for approving access to the system being requested.

(19c) Date. The date the ISSO or Appointee signs the DD Form 2875.

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

C. PART III: Verification of Background or Clearance.

(22) Type of Investigation. The user's last type of background investigation (i.e., Tier 3, Tier 5, etc.).

(22a) Investigation Date. Date of last investigation.

(22b) Continuous Evaluation (CE) Deferred Investigation. Select yes/no to validate whether or not the user is currently enrolled for "Deferred Investigation" in the Continuous Evaluation (CE) program.

(22c) Continuous Evaluation Enrollment Date. Date of CE enrollment. Leave blank if user is not enrolled in CE.

(22d) Access Level. The access level granted to the user by the sponsoring agency/service (i.e. Secret, Top Secret, etc.). Access level refers to the access determination made on the basis of the user's individual need for access to classified information to perform official duties; a determination separate from the user's eligibility determination.

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

(24) Phone Number. Security Manager's telephone number.

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

(26) Verification Date. Date the Security Manager performed the background investigation and clearance information verification.

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 e CONTROLLED UNCLASSIFIED INFORMATION" 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 ISSO. Recommend file be maintained by ISSO adding the user to the system.