

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional Information)

If you are requesting SIPRNet access, you are **PERMANENT PARTY** to **ARNORTH**, and you do not have a SIPRNet token, go to: <https://portal.arnorth.army.mil/cs/g6/itsd/cs/Lists/str/Pending.aspx> to request one or get with your Supervisor for assistance.

If you are **NOT PERMANENT PARTY** to **ARNORTH** and do not have a SIPRNet token, you will need to get with your organization to order one. If that is not possible, get with your ARNORTH SPONSOR for assistance.

If you have an existing SIPRNet token, the certificates on it are good for a total of 3 years.

TYPE OF REQUEST:

SSN:

EDIPI:

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 LEVEL I LEVEL II LEVEL III	
29. VERIFIED BY (Print Name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)

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)

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 Email Address. The user's official email address.
- (6) Job Title and 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. (Active Duty, Reservist, National Guard, Civilian, or Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed 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 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.
- (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 sign the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) Email Address. Supervisor's email 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 sign 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 sign the DD Form 2875.
- (27) Optional Information. This item is intended to add additional information, as required.

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