DD2875 SAAR Instructions

Overview

The DD2875 SAAR is required to obtain access to the Advana platform. All users should submit their complete DD2875 to the service desk via an access request ticket the first time they are requesting access to anything on the Advana platform. Instructions on how to submit an access request ticket are documented in the **Advana Service Desk User Guide**. Instructions on how to complete the DD2875 are explained below.

Download a Template Advana SAAR Form

Part I - Administrative Data

Part I of the SAAR includes administrative data from the user requesting Advana access. **They must enter their DoD ID in the User ID box.** The remainder of the SAAR is completed as follows:

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).

> Foreign Nationals must submit a memo waiver to the Service Desk. **Click here for guidance on Foreign National Citizenship Waivers.**

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. The completion date must be current within 1 year of being signed by all parties.

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). The signature must be digitally signed with a CAC. Invalid/wet signatures will not be accepted.

12. Date: The date that the user signs the form.

Part II - Supervisory Endorsement of Access

Part II of the SAAR encompasses the endorsement and justification for the user requesting access. **It requires the endorsement and digital signature of the user's supervisor.**

> ⓘ Please note that block 21 and 22 of the SAAR must remain unsigned. These blocks are completed by an Advana staff member. If invalid signatures are found in these fields, the SAAR will be rejected by the Service Desk.

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.

> Unclassified - Individual requesting access to Advana on NIPR
>
> Classified - Individual requesting access to Advana on SIPR

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

> **16a. Expiration Date for Access:** Contractors must enter their contract # and expiration date in this field.
>
> If the user is CIV or MIL please mark N/A.

17. Supervisor's 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. The signature must be digitally signed with a CAC. Invalid/wet signatures will not be accepted.

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: Signature of the functional appointee responsible for approving access to the system being requested. This block is left blank. If this block is completed it the SAAR will be rejected by the Service Desk.

> ⚠ Block 21 no longer needs to be signed by Agency gatekeepers for **NFR Database** access.

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. This block is left blank. If this block is completed, the SAAR will be rejected by the Service Desk.

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. Product Specific Access Only: Field is left blank.

Part III - Certification of Background Investigation

Part III of the SAAR is completed by the user's security officer. The purpose of this portion of the SAAR is the verify and certify the user's background investigation information. **It requires the digital signature of the user's security officer.**

28. Type of Investigation: The user's last type of background investigation (i.e., NAC, NACI, or SSBI). If none, enter "NONE."

28a. Date of Investigation: Date of last investigation.

28b. Clearance Level: The user's current security clearance level (Public Trust, Secret or Top Secret). If none, enter "NONE."

28c. IT Level Designation: The user's IT designation (Level I, Level II, or Level III), if applicable. If none, leave blank.

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. The signature must be digitally signed with a CAC. Invalid/wet signatures will not be accepted.

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

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)

Related articles

- DD2875 SAAR Instructions
- Service Desk Access Forms