

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 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 <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____		DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications)		LOCATION (Physical Location of System)

PART I (To be completed by Requestor)

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 <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information 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 REQUIRED: <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER _____			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
17. SUPERVISOR'S NAME (Print Name)		18. SUPERVISOR'S SIGNATURE	
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT		20a. SUPERVISOR'S E-MAIL ADDRESS	
21. SIGNATURE OF INFORMATION OWNER/OPR		21a. PHONE NUMBER	
22. SIGNATURE OF IAO OR APPOINTEE		22b. DATE (YYYYMMDD)	
23. ORGANIZATION/DEPARTMENT		24. PHONE 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 <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> 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 FOR THE DPAS DD FORM 2875

The following instructions have been modified. The original standard instructions for filling out the DD 2875 are in non-bold type. **All instructions specifically for DPAS Users are in bold.** Each user will be required to complete/provide:

- 1.) **DD Form 2875**
- 2.) **A User Agreement showing the user has read and agrees to the rules**
- 3.) **A current Information Awareness or Cyber Awareness Challenge certificate of completion**
- 4.) **A DPAS Roles Request Form detailing the users access for the appropriate module. Typically this form is completed by the users Accountable Property Officer (APO) or Information Owner (IO).**

DPAS user access forms are located at <http://dpasupport.golearnportal.org/>. As of May 14, 2012, all user access forms must be digitally signed by all parties and are required to be the original PDF documents found on the DPAS Support website. Exceptions to this rule will be made on a case-by-case basis. If an exception is made, a faxed or scanned copy may be permitted. Hard copies sent through the mail will only be accepted as a last resort. If an exception is made, please know nothing can be scratched out and there cannot be any markings that could be interpreted as an alteration of the original form or its contents.

IMPORTANT: This form contains Personally Identifiable Information (PII) with a low confidentiality impact level. In order to properly protect the information, this form must be encrypted if being sent via email. In lieu of emailing the form, it is recommended internal share drives be used to obtain the signatures required for proper completion.

Pre-filled fields are only applicable when using the DPAS 2875 wizard.

All blocks in Part I, II and III are mandatory except blocks 16a for Civilians and Military personnel and blocks 22, 23, 24 and 25.

Type of Request: Select "Initial" for new access requests. Select "Modification" for a name change. Name changes require a new user packet to be submitted. Select "Deactivate" for account deletions.

Date: Enter the "Date" of request. This date should be the oldest date on the form. Date must be in the proper YYYYMMDD format.

System Name (Platform or Applications): Pre-filled with "DPAS"

Location: Pre-filled with "DECC OGDEN"

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

- (1) **Name:** Enter the last name, first name, and middle initial of the user.
- (2) **Organization:** Provide the user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (3) **Office Symbol/Department:** Provide the office symbol within the current organization (i.e. SDI). **Enter your Government Office Symbol.**
- (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 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:** Provide the user's official mailing address.
- (8) **Citizenship:** (US, Foreign National, or Other).
- (9) **Designation of Person:** (Military, Civilian, or 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 IA Training has been renamed to Cyber Awareness Challenge. The DoD requires this training be completed annually. Refresher training completion must be verified by the user annually to retain access to the application. It is recommended the training be completed prior to submitting the DD Form 2875. If not, the training date provided must be within the past 11 months. This will allow 30 days for the completion of the form and processing. If the date has expired before the form is processed, proof of course completion will be required.**
- (11) **User 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 user's digital signature must be present before sending to the supervisor for completion of Part II. The date included in the digital signature must match the date in block 12.**

- (12) **Date:** The date that the user signs the form. **The date must be equal to or greater than the date in the upper right hand corner of page one. The dates must be equal to or less than the dates in blocks 18, 19, 21, 21b, 31 and 32. The date must be in the proper YYYYMMDD format.**

Part I must be completed in its entirety before sending to the Supervisor to complete Part II.

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. **If an exception is made and the user hand signs the form or the users EDI number is not included in the digital signature, then the user's Electronic Data Interchange (EDI) number must also be provided.**
- (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.) **Pre-filled with Authorized. If Privileged access is required, a manual change is necessary before saving the form.**
- (15) **User Requires Access To:** Places an "X" in the appropriate box. Specify category. **Pre-filled with Unclassified.**
- (16) **Verification of Need to Know:** To verify that the user requires access as requested. **Must not be left blank.**
- (16a) **Access Expiration Date.** The user must specify expiration date if less than 1 year. **If the user is a contractor, the Company Name, Contract Number and Expiration Date must be provided. Use Block 27 if needed.**
- (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. **The supervisor's digital signature must be present before sending to the Security Manager for completion of Part III. The date included in the digital signature must match the date in block 19.**
- (19) **Date:** Date the supervisor signs the form. **The supervisor must sign the form after the user but before the Security Manager and Information Owner. In other words, the dates in blocks 11 and 12 must be equal to or less than the dates in blocks 18 and 19. The date must also be equal to or less than the dates in blocks 21, 21b, 31 and 32. The date must be in the proper YYYYMMDD format.**
- (20) **Supervisor's Organization/Department:** Supervisor's organization and department.
- (20a) **Supervisor's Email address:** Supervisor's email address.
- (20b) **Phone Number:** Supervisor's telephone number.

INSTRUCTIONS FOR THE DPAS DD FORM 2875

Blocks 21, 21a and 21b are reserved for the pre-appointed DPAS Information Owner (IO), Alternate Information Owner (AIO), Functional Data Owner (FDO) or Alternate Functional Data Owner (AFDO).

(21) *Signature of Information Owner/OPR:* Only complete if Part I, II and III have all been completed properly. The DPAS appointee's digital signature must be present. The date included in the digital signature must match the date in block 21b.

(21a) *Phone Number:* Functional appointee telephone number.

(21b) *Date:* The date the functional appointee signs the DD Form 2875. **The date the DPAS appointee digitally signed block 21. The date must be in the proper YYYYMMDD format. The date must be the last date on the form before sending to DPAS Account Management.**

Blocks 22, 23, 24 and 25 must be blank. They are reserved for DPAS Account Management.

(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.

(26) *Name:* Pre-populated from block 1.

(27) *Optional Information.* This item is intended to add additional information, as required. **If the contract of a Foreign National is in compliance with the Status of Forces Agreement (SOFA) it must be noted in either block 27 or 13. Foreign Nationals must also provide their country of citizenship.**

Part II is complete, send to the Security Manager for completion of Part III.

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

SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

For government employees, the Security Manager will be the Local Government Security Officer.

For contractor employees, the Security Manager will be either the Local Government Security Officer or the contractor's company security officer.

By completing Part III, to include signing Block 31, the Security Manager is attesting to the validity of the information supplied in Blocks 28, 28a, 28b, and 28c. DoD regulations require a background investigation (at a minimum NAC/NACLC) for government and contractor employees.

(28) *Type of Investigation:* The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) *Date of Investigation:* The date of last investigation.

(28b) *Clearance Level:* The user's current security clearance level (Secret or Top Secret). **The Security Manager will enter the determined clearance from the investigation. If the user does not have a clearance, "NONE" should be indicated.**

(28c) *IT Level Designation:* The user's IT designation (Level I, Level II, or Level III). **The Security Manager will enter only one IT level designation resulting from the investigation.**

(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 Security Manager's digital signature must be present. The date included in the digital signature must match the date in block 32.**

(32) *Date:* The date that the form was signed by the Security Manager or his/her representative. **The date must be equal to or greater than the dates in blocks 11, 12, 18 and 19. The date must be in the proper YYYYMMDD format.**

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.

The DD Form 2875 contains low confidentiality level PII. If the form is sent via email, it must be encrypted. If encrypted share drives are available within your agency, saving the form to a share drive for the required parties to access and complete is recommended.

Completed user access forms must be sent to the DPAS appointed IO, AIO, FDO or AFDO for final review/approval. Once approved, the forms must be uploaded to the appropriate DFAS ePortal project. If submitting forms for a new user, the forms required are the DD Form 2875, User Agreement, Roles Request Form and the Information Assurance or Cyber Awareness Challenge training certificate. If changing users existing access, only a Roles Request Form detailing the appropriate changes is required. Any questions can be addressed via email to cco-dpas2875@dfas.mil.