DLA Information Operations
"How To" Guide

OPR: J64DACA

How to Complete A DD2875 for Access to DLA Systems

This How to Guide provides you step by step instructions on how to complete a DD2875 to request access to DLA systems. The DD2875 is required when a system is not in the DLA Account Management and Provisioning System (AMPS) and when access to external DOD systems is required.

1) The latest version of the DD2875 can be found here.
2) The latest version of the Consent to Monitor, Privileged Rules of Behavior can be found here. ***Please work with Michele to get them on the J6 webpage or someplace appropriate.
3) Cyber awareness training and PII Training for users without a CAC can be found here.

After you have completed the forms, please submit your access request to the Enterprise Helpdesk (EHD) https://ehdselfservice.ad.dla.mil. The table below indicates which blocks are required for the different types of access requests:

****If there is a better way to capture it, go for it.

	Normal User Access (IT III)	Privileged Access (IT I or IT II)	Employee Transfer	Employee Deactivation
"Type of Request"	X	X	X	X
"System Name"	X	X	X	
"User ID"	X	X	X	X
Part 1, 1-12	X	X	X	
Part 2, 13-27	13-21b. required	13-21b. required	13-21b. required	13-21b. required
Part 3	EX	X		
Rules of Behavior	DLA/EX			
PII Training	DLA/EX	DLA/EX		
Cyber Awareness Training	DLA/EX	DLA/EX		
Privileged Rules of Behavior		X		

X = Required by All Users
EX = Required by Non DLA Users (Copy of Certificate needed)
DLA = Required by DLA Employees at Onboarding not needed for paper process

FORM INSTRUCTIONS:

4) Type of Request: Indicate the type of request. Select "Initial" if this is the first request for a particular system. Select "Modification" if a change to existing access to a system is being requested. Select "Deactivate" if the employee is leaving DLA or no longer requires access to the system.
5) User ID: Enter the employee's user ID
6) Date: Enter the date the DD2875 is filled out.
7) System Name: List the system for which access is being requested.
8) Location: This field is optional. If the location is germane to the request, please include it.

Form Part I:

1) Block 1: Enter the name of the employee for whom access is being requested.

2) Block 2: Enter the organization of the employee. For example, “DLA Land & Maritime,” “DLA Information Operations,” or “DLA Distribution.”
3) Block 3: Enter the office symbol or department. For example, “J63BA.”
4) Block 4: Enter a phone number where the employee can be contacted.
5) Block 5: Enter the official (government, military, or commercial) e-mail address of the employee for the entity they are requesting access for. (Example: If military use military email, Do not submit as a DLA employee using your military email)
6) Block 6: Job Title and Grade/Rank: Job title and rank, i.e., IT Specialist, GS-12, or Regional Director, LTC, USAF.
7) Block 7: Official mailing address: enter the postal address of the employee’s office/worksite location.
8) Block 8: Please check the appropriate citizenship block for the employee: US citizen, Foreign National, or Other.
9) Block 9: Check if employee is civilian, contractor, or military.
10) Block 10: IA Training and Awareness Certification Requirements: Mark to indicate if the DOD Cyber Awareness Training has been completed and the date the training was completed. If the training was taken external to DLA, please include a copy of the completion certificate with the 2875.
11) Block 11: User Signature: User Signature is optional; the supervisor may sign on behalf of the user. If the user requesting access is external to DLA, the End User Rules of Behavior must be signed by the user and included with the 2875.
12) Block 12: Date: Date form is signed.

Form Part II:

1) Block 13: (“Justification”) Please enter a brief justification of the requirement.
2) Block 14: If a special type of access is required, please mark the appropriate type. For IT III / routine access level, mark Authorized Access. For IT I and IT II level of access, mark Privileged Access.
3) Block 15: If the employee requires specific security level access to the system, place a mark in the appropriate box and indicate the category, i.e., SIPRNet, etc.
4) Block 16: Verification of Need to Know: The supervisor/representative (Representatives are government employees) will mark the box certifying that the employee requires access as requested.
5) Block 16A: For contractors requiring access, they must specify company name, contract number, and expiration date. Use block 27 if additional space is required. The expiration date is the expiration of the entire contract.
6) Block 17: Enter the supervisor’s/representative’s name (typed or printed) in block 17.
7) Block 18: The supervisor’s or representative’s (COR for Contractors) signature is require.
8) Block 19: Enter the date signed.
9) Block 20: Supervisor’s Organization/Department: Enter supervisor’s office symbol.
10) Block 20a: Enter the government email address of supervisor/representative.
11) Block 20b: Enter the phone number of supervisor/representative.
12) Block 21: Signature of Information Owner/OPR, Also known as the Data Owner: The Information Owner is the last signer of the 2875. The Information Owner is approving the access and validating that the user has need to know and meets access requirements of the role being requested. Digital signature is acceptable.
13) Block 21a: Enter the phone number of Information Owner.
14) Block 21b: Enter the date of signature of the Information Owner.
15) Block 22: Signature of IAO or Appointee: *Not Required per CIO Guidance*.
16) Block 23: Organization/Department: *Not Required per CIO Guidance*.

17) Block 24: Phone Number: *Not Required per CIO Guidance*.
18) Block 25: Date: *Not Required per CIO Guidance*.
19) Block 26: Enter the name of the employee.
20) Block 27: Optional Information: Use this box to include any additional information that the Information Owner or account provisioners will need for approving/granting the access.

Form Part III:

1) This section is to be completed by the Security Manager (DLA DI) or representative for Privileged (IT I and IT II) access, NIPR PRIV access and SIPRNet access requests. All external users requesting a role requiring an IT Level must signed.
2) Block 28: Enter the type of background investigation on record for the employee.
3) Block 28a: The date the investigation was completed should be entered.
4) Block 28b: The level of clearance on record for the employee should be entered.
5) Block 28c: The IT Level designation the employee is approved for should be entered.
6) Block 29: Enter the name of the verifying Security Manager.
7) Block 30: Enter the phone number of Security Manager.
8) Block 31: The Security Manager's signature is required.
9) Block 32: Enter the date the Security Manager signed the form.

Form Part IV: For use by CS I&AM Only.

Additional Questions?

http://iatraining.disa.mil/eta/piiv2/launchPage.htm
http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm

Contact the Enterprise Help Desk:

Call: 855-352-0001
Email: DLAEnterpriseHelpDesk@DLA.mil
Website: https://ehdportal.ad.dla.mil/