

Information Owner & Alternate Information Owner Guide



Defense Logistics Agency (DLA)
Logistics Catalog and Data Solutions (LCDS)



1. Introduction.....	3
2. Responsibilities of ELMS IOs/AIOs.....	4
3. ELMS Access Request Instructions.....	6
4. DoD Cyber Awareness Challenge Certificate Requirements.....	9
5. Role Request Form Requirements.....	10
6. User Agreement Form Requirements.....	12
7. SAAR-DD2875 Form Requirements.....	13
8. SAAR-DD2875 Form Breakdown.....	14
9. Common Reasons for User Access Request Packet Return.....	15
10. IO Retroactive User Activity Investigation.....	16
11. For More Information.....	18



Congratulations! You have been appointed as an Enterprise Logistics Management System (ELMS) Information Owner (IO) or Alternate Information Owner (AIO). You are now authorized to sign for ELMS user access requests. The information provided in this webinar will guide you through your new responsibilities and any paperwork processes necessary for new user access requests.

Any questions regarding your IO/AIO appointment, CCB designation, or new user accounts, please contact ELMS Account Management by emailing ELMSSecurity@leidos.com. Any questions regarding training accounts, eLearning support, ELMS log in errors, etc., please contact ELMS Support by emailing ELMSSupport@leidos.com or by calling 1-844-843-3727. Further information on the ELMS system is outlined on our support site: <https://elmssupport.golearnportal.org>.

You are now authorized to sign for user access to the ELMS tiers in which you are appointed. You may sign for user update access up to your appointed tier level and all levels that fall below. Only IOs that are also CCB Members can sign for tier level access requests higher than their appointed tier level.

- You must maintain an active ELMS Production account.
- You will verify that roles being assigned to the user do not conflict with other duties or actions within ELMS or other systems per Separation of Duties (SOD).
 - A list of roles can be found on our support site by hovering over 'System Solutions', hovering over 'By Role', and selecting the module.
- You will review all user forms prior to submission to ensure all are completed in their entirety and fields are entered correctly.
 - User form requirements start on page 9.
- You will upload user access request packets, following instructions outlined on pages 6-8.
- You will send a digitally signed email to ELMSSecurity@leidos.com confirming when a user no longer requires access, requesting account deletion.
- You will send a digitally signed email to ELMSSecurity@leidos.com confirming a user's new contract information, designation (MIL/CTR/CIV) change, name change, or email change.

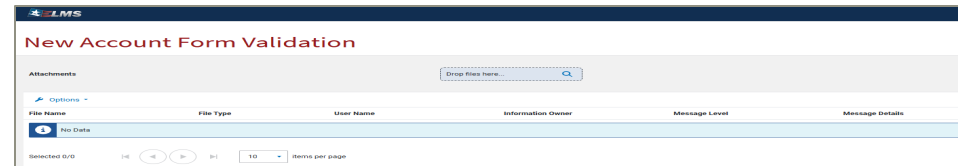
- You will review IO/AIO appointments throughout the year to ensure those signing for user access are still valid per their designation.
 - A full IO listing may be requested by emailing ELMSSupport@leidos.com.
 - Send a digitally signed email to ELMSSecurity@leidos.com if IO/AIO removal is required or if an appointment form is needed to add an additional appointee.
- When necessary, you will log a ticket with ELMS Support requesting a Retroactive User Activity Investigation and follow instructions outlined on pages 16-17.
 - This is necessary if a user has access to ELMS longer than required, or if you suspect a user has negatively impacted ELMS data.
- You will perform an Annual User Access Review (UAR) each year, initiated when an email is sent by the ELMS Account Management Team including instructions and the UAR due date.
 - The User Access Inquiry role assists you in generating user listings for review.
 - A review form is included in the email for you to complete and return after user review is finalized.
 - All larger IO groups are to coordinate their responses through the main IO to reduce duplication.
 - If an Annual Review form is not received from a group, this may result in users being put into a suspended status until a completed review form is received.
 - Retain all supporting annual review documents for internal organization audit(s).

All user forms submitted MUST be current forms downloaded from the ELMS Support site.

- Visit <https://elmssupport.golearnportal.org/>.
- Hover over 'Support', select 'Request Access', and select the ELMS module the user is requesting access to.
- Review the 'Download the Forms', 'Understand the Forms', and 'Submit the Forms' information.
- Select on each user form link, downloading the form and saving it to your desktop using the required naming convention for consistent archiving and querying capability.
 - Last Name First Name MI Form Name
 - Example: Smith Jane L 2875
 - If user has no middle name, use NMN
 - Example: Smith Jane NMN 2875
- Save all four completed forms as PDF files within one folder on your desktop.
 - Use Adobe Acrobat for review, completion, and signing of the forms to prevent format and processing errors.
 - Processing errors may also occur due to an individual's computer settings.
 - If you discover this is the issue, it must be addressed with your local Information Technology (IT) administrators(s).
 - Forms must be saved as PDF files to process successfully.
 - Right click on the Folder, hover over 'Send To', select 'Compressed (zipped) Folder', and name the zip file using the required naming convention outlined above.

All user forms MUST be reviewed for accuracy and completeness prior to submitting for processing.

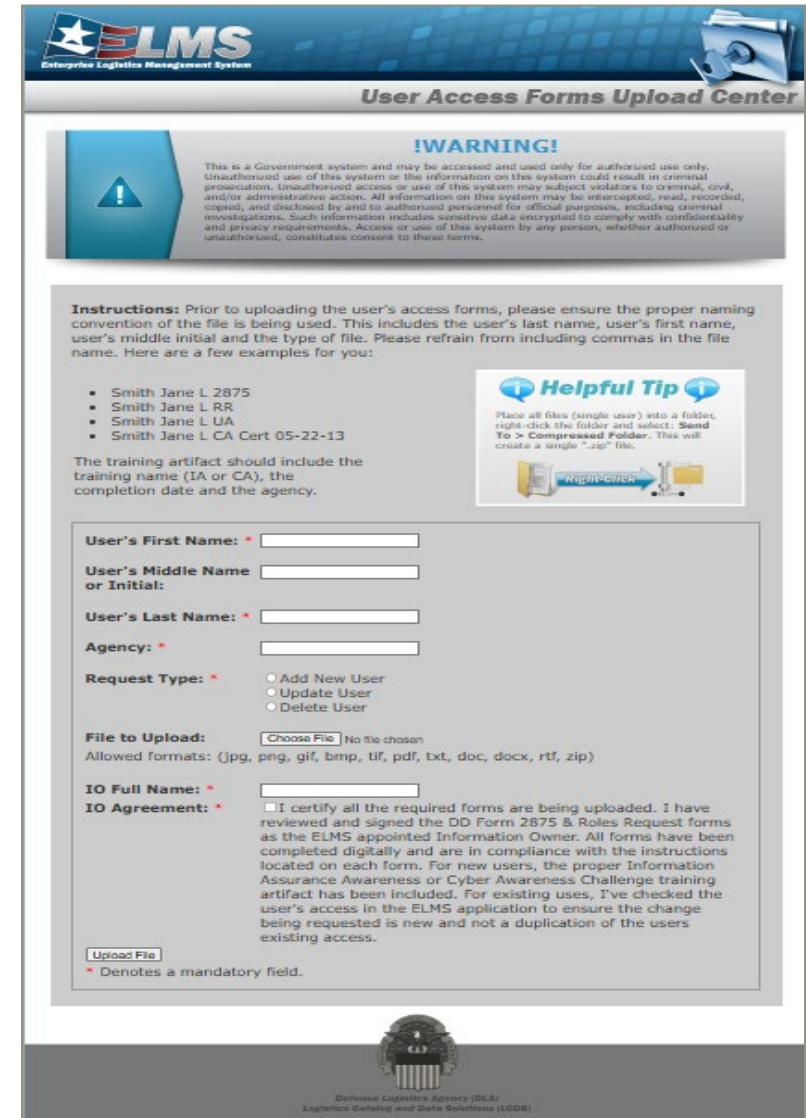
- Access the web validation tool to assist with form review by visiting <https://prod.elms.dla.mil/new-accounts>.



- Drag and drop a single form or zipped form packet into the 'Drop files here' box at the top of the screen OR select the magnifying glass to search and select files.
- The validation tool will review and return results, listing each individual form's validation status.
 - Confirms if the form completion is a success.
 - Provides a warning or error if a form needs additional review and correction before submission.
- The tool is for validation purposes only and is not tied to an ELMS account, nor does it load user information into the system.
 - Manual review is necessary for Role Request (RR) forms received for the ELMS Force Systems Management (FSM), Material Management (MM/ICP), and Registry modules.
 - The system has not yet been programmed to complete review of RRs for these modules.
 - Manual review will be needed to verify the date and correct training name on the DoD Cyber Awareness Certificate.
 - All 2875 date format variations and investigation types may not be included within the validation, and some formats may still generate an error even when valid.
 - ELMS Security will accept the forms if the dates are listed as complete calendar dates and investigation types are valid.
- Once user forms are reviewed and validated successfully, the IO/AIO will upload them for processing.

To upload user forms for processing:

- Access the User Access Forms Upload Center by visiting <https://elmselearning.golearnportal.org/fileupload/useraccess.php>.
- Enter the user's First Name, Last Name, and Agency.
- For request type:
 - Select 'Add New User' for a new account creation.
 - Select 'Update User' for updating an existing account.
 - Selection of 'Delete User' is not applicable.
 - The IO should instead send a digitally signed email requesting ELMS user account deletion to ELMSSecurity@leidos.com.
- Browse and select the file for upload.
- Enter the IO Name and check the IO Agreement.
- Upload the file.
- User files received will be downloaded and then removed from the secure upload site.



The screenshot shows the 'User Access Forms Upload Center' interface. At the top is the ELMS logo and a 'WARNING!' banner with a disclaimer. Below this are 'Instructions' regarding file naming conventions and a 'Helpful Tip' about file compression. The main form contains fields for 'User's First Name', 'User's Middle Name or Initial', 'User's Last Name', 'Agency', and 'Request Type' (with radio buttons for 'Add New User', 'Update User', and 'Delete User'). There is a 'File to Upload' section with a 'Choose File' button and a list of allowed formats. Below that is the 'IO Full Name' field and the 'IO Agreement' section, which includes a checkbox for certifying that all required forms are being uploaded and a detailed statement of agreement. An 'Upload File' button is at the bottom left of the form area. A footer at the very bottom displays the Department of Defense seal and the text 'Defense Logistics Agency (DLA) Logistics Catalog and Data Solutions (LCDS)'.

The training certificate must include:

- The full name of the person that completed the training.
- The full name of the training.
- The training completion date.
 - Training completion must be dated within the past year.

An example of the DoD Cyber Awareness Challenge Certificate:



- The form must be a current form downloaded from the ELMS Support site.
- Role Request (RR) Forms are used to request new ELMS access or to update existing access.
 - For updates to existing access, complete all necessary fields and note a reason for the update within the 'Additional Information' section.
 - Only a role form is needed for updates if the user has an existing account.
 - A single form submission does not need to be zipped.
- For new access requests, there must be at least one RR form included in submission.
 - Multiple RR forms can be included if the user needs access to multiple system locations.
- Roles are to be selected per the user's needs.
 - For role descriptions, visit the ELMS Support site, hover over 'System Solutions', hover over 'By Role', and select the system module.
 - The IO Role cannot be assigned to a user who hasn't been appointed as an IO.
 - A contractor cannot carry an Accountable Property Officer (APO) role and must instead request the combination of Property Administrator (PA) and Catalog Manager roles.
 - A Property Accountability (PA) RR Form requires a CCB Signature if the IO signing is not appointed for Agency, is not a CCB Member, and is requesting an update role at Agency level.
- Access Tier name(s) being requested must already exist within ELMS and be spelled exactly as presented within the system.
- An example of a PA RR form is provided on the next slide.

Role Request Form

Signatures:	
*User Signature only required if EDIPI is not listed above *If IO & CCB are the same, only one signature is required in IO field.	
Signature of ELMS User:	<div> <div>Signature</div> <div></div> </div> <div> <div>Date:</div> <div>Today</div> </div>
Signature of Information Owner:	<div> <div>Signature</div> <div></div> </div> <div> <div>Date:</div> <div>Today</div> </div>
Signature of CCB Member:	<div> <div>Signature</div> <div></div> </div> <div> <div>Date:</div> <div>Today</div> </div>

Role Request Form

Extra Assignments:			RESET ASSG.
Actbl UIC	UIC	Custodian	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	
<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	<div><div></div>All <input type="checkbox"/></div>	

Role Request Form

All user access forms are located on the ELUMS Support website at <http://ELUMSsupport.golearnportal.org/>. Once on the page go to Support > Request Access > and then select Property Accountability.

To view all available Roles and associated training, click the [View ELMS Roles Spreadsheet](#)

User Name	Required	<ul style="list-style-type: none"> • Enter in the necessary fields.
User's EDIPI	Optional	<ul style="list-style-type: none"> • Enter the User's EDIPI if the User's signature is not present.
Agency	Required	<ul style="list-style-type: none"> • Only one Agency is permitted per form.
Site-ID	Required	<ul style="list-style-type: none"> • Only one Site-id is permitted per form unless the user requires access to All Site-ids. In this case, check the ALL checkbox.
Environment	Required	<ul style="list-style-type: none"> • One Environment must be selected from the drop-down menu.
Form Type	Required	<ul style="list-style-type: none"> • Select the purpose of the form, to update or create a user's account.
Manager	Optional	<ul style="list-style-type: none"> • Currently only used by the Navy. • Selection determines the results of the UICs with Assets with no owners Agency Pre-Defined Inquiry.
Level of Access	Required	<ul style="list-style-type: none"> • Level of Access will determine where the roles are assigned. • Indicate which level of access is required for each: Update, Reports, and Inquiry. • Update roles at Agency level require COB signature
Actbl UIC(s)	Required	<ul style="list-style-type: none"> • If Level of Access for updates is Site or above, then check the ALL checkbox for Actbl UIC & UIC combination. • If Level of Access for updates is equal to Actbl UIC, then enter a valid Actbl UIC/ UIC Combination. • Access may be requested for one or more valid Actbl UIC(s) per Associated Site-id. • If multiple Actbl UICs are requested for a specific Site-id, List each on a separate line. (More space is on page 2).
UIC(s)	Required	<ul style="list-style-type: none"> • If Level of Access for updates is Actbl UIC or above, then check the ALL checkbox for UIC and enter valid Actbl UIC. • If Level of Access for updates is equal to UIC, then enter a valid Actbl UIC/ UIC Combination in corresponding fields. • Access may be requested for one or more valid UIC(s) per Associated Site-id/Accountable UIC Combination. • If multiple UICs are requested for a specific Actbl UIC, List each on a separate line. (More space is on page 2).
Custodian(s)	Required	<ul style="list-style-type: none"> • If Level of Access for updates is UIC or above, then check the ALL checkbox for Custodian. • If Level of Access for updates is equal to Custodian, then enter a valid Actbl UIC/ UIC/Custodian combination in the corresponding fields. • Must be Custodian number NOT the Custodian name.
Role Selections	Required	<ul style="list-style-type: none"> • Select the desired roles from the drop-down menu and indicate Add or Delete. • If Accountable Property Officer (APO) is selected, user must be a government employee designated in writing – Can't be a contractor. • The Agency Report and Forms Generation role can only be selected if the Users Level of Access for Updates, reports and Inquiry is equal to Agency. This will provide user access to the CFO Accounting Report and the Acquisition Program CIP Project Status report. If these reports are not needed, the role should not be assigned.
Additional Information	As needed	<ul style="list-style-type: none"> • Include any Additional Information that can assist with the Update process.
Signature of ELMS User & Date	Required	<ul style="list-style-type: none"> • Required if User's EDIPI is not present above. • Include the digital signature with EDIPI # of the User who is requesting access to the ELMS System. • Enter the date the form is digitally signed.
Signature of Information Owner & Date	Required	<ul style="list-style-type: none"> • Include the digital signature of the appointee responsible for approving access to the ELMS system. (i.e. Information Owner or Alternate Information Owner). • Enter the date the form is digitally signed
Signature of CCB Member & Date	Optional	<ul style="list-style-type: none"> • If the user is assigned the 'Agency Coordinator' or an update role at Agency level, then this field is required. If the IO and COB member is the same person, only one signature is required in the IO field.

User Agreement Form Requirements

UNCLASSIFIED // FOR OFFICIAL USE ONLY

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.
- You consent to the following conditions:
 - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 - At any time, the U.S. Government may inspect and seize data stored on this information system.
 - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
 - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
 - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

Signature/Date _____

- The form must be a current form downloaded from the ELMS Support Site.
- User must read and digitally sign the bottom of the form using their federally issued PKI cert.
 - Digital signature must be an active box that can be clicked on to verify and must be dated within the past year.
 - In rare cases, ELMS Security may approve use of a handwritten signature and handwritten date instead of a digital signature ("wet-signed").
- Scanned forms are not accepted and will be returned.

SAAR-DD2875 Form Requirements

- The form must be a current form downloaded from the ELMS Support site.
- Digital Signatures must be:
 - Completed using a federally issued PKI cert and must have the EDIPI present within the signature.
 - Dated within the past year.
 - IO signature must be current and not reused.
- Signature order by date/time stamp (time zones must be considered):
 - User's Signature is first to initiate request.
 - Supervisor's signature
 - Security Manager's signature
 - IO or AIO Signature is last to authorize the account.
- Type of Request
 - New users = Initial Request
 - YYYYMMDD = Date
 - System Name = ELMS
 - Location = DLA Cloud

UNCLASSIFIED

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 this burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at wha-mc-alex-and-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		DATE (YYYYMMDD)
<input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____		
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 <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 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 <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 <input type="checkbox"/> I certify that this user requires access as requested.	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 21 if needed.)	
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		

UNCLASSIFIED

DD FORM 2875, MAY 2022 PREVIOUS EDITION IS OBSOLETE. Page 1 of 3

UNCLASSIFIED

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)		

UNCLASSIFIED

DD FORM 2875, MAY 2022 PREVIOUS EDITION IS OBSOLETE. Page 2 of 3

- Part I – User Section: Boxes 1-11 must be complete.
 - Box 10 = date of the DoD Cyber Awareness certificate being included within the user packet.
 - Must be within the past year.
- Part II – Supervisor Section: Supervisor reviews all prior sections to ensure data is complete and accurate.
 - Boxes 13-17d must be complete.
 - Box 14 = Authorized
 - Box 15 = Unclassified
 - Box 16 must be checked
 - Box 16a needs completed for CONTRACTORS ONLY and must be in the following format for processing:
 - Company Name, Contract Number, YYYYMMDD
- Part III – Security Manager Section: Security Manager reviews all prior sections to ensure data is complete and accurate.
 - Boxes 22-25 must be complete.
 - A user must have an investigation complete or, in the very least, initiated.
 - If a user does not have a Clearance Level, 'NONE' can be listed for Access level.
- IO/AIO Section: the IO/AIO reviews all prior sections to ensure they were completed in the correct order.
 - Boxes 18 and 18a must be complete.
 - The IO/AIO is the last digital signature, which authorizes account creation before uploading the request for processing.
- ELMS Account Management Section: Boxes 19-19b are reserved for ELMS Account Management completion.
 - If Boxes 19-19b are not left blank for Security Officer completion, the user account request packet will be returned to the submitting IO.

- The form was scanned or has been altered and cannot process.
- All four user request forms are not included within the zipped user packet.
- The Cyber Awareness Certificate provided is not for the DoD Cyber Awareness Challenge, does not list the full name of the user requesting access, or is not dated within a year.
- Incomplete or incorrect form fields on one or all forms.
 - The 'System Name' is not listed as 'ELMS' on the SAAR-DD2875.
 - The 'Location Name' is not listed as 'DLA Cloud' on the SAAR-DD2875.
 - The digital signatures are not in proper order on the SAAR-DD2875.
 - The digital signatures cannot be selected for verification.
 - The access tier requested on the RR Form does not match the tier name within ELMS.
 - The person signing as IO on the form(s) is not an appointed IO/AIO.
 - The person signing as IO on the form(s) is also the user requesting access on the form.
 - The Security Manager signing for Part III and the IO that has signed are the same person.
 - The Security Manager must be a separate person than the IO due to Separation of Duties (SOD).
 - Digital signature error on any of the forms.
 - In rare cases, ELMS Security may approve use of a handwritten signature on the UA instead of a digital signature ("wet signature").
 - In these cases, the form date must also be handwritten.

If an IO/AIO identifies a user who had access to ELMS and did not require it, or negative impact to ELMS data is suspected, these Retroactive User Activity Investigation Steps will be conducted by the IO/AIO to support the investigation of incidents outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The investigation will identify whether the user activity meets one of the following insider threat categories:

1. Sabotage = The insider uses their legitimate access to damage or destroy organizational systems or data.
2. Fraud = The theft, modification, or destruction of data by an insider for the purpose of deception.
3. Intellectual Property Theft = The insider steals the organization's intellectual property, often for resale or to take with them to a new position.
4. Espionage = The insider threat is stealing information for another organization, such as a competitor, government, etc.

The IO will begin the investigation by running and reviewing an ELMS Accounting Transaction Inquiry to verify if the user under investigation conducted questionable actions.

- Log into the ELMS Property Accountability (PA) module.
- Hover over 'Inquiries', hover over 'Accounting' and select 'Accounting Transactions'.
- Using the Available Fields dropdown, select 'Estbd Dt', select <= as the operand, and enter a date that is prior to or equal to the first date of departure.
 - Utilize the 'Fields' button if you would like to receive further information within the data retrieval.
- Select 'Show Inquiry' and the Accounting Transactions Inquiry will populate.
 - If there are rows returned for the person's User Id and all are acceptable, then the investigation can be concluded.

If there are rows returned for the person's User Id that identify unauthorized system activity, the IO will continue the investigation by:

- Sending a digitally signed email to ELMSSecurity@leidos.com requesting immediate user access removal.
- Running and reviewing an ELMS Asset Activity Inquiry to verify if the user under investigation conducted any further questionable actions.
 - Log into the ELMS PA module, hover over 'Inquiries', hover over 'Asset Management', and select 'Asset Activity'.
 - Enter a Transaction Dt to start from and the User Id of the user being investigated.
 - Utilize the 'Fields' button if you would like to receive further information within the data retrieval.
 - Select 'Show Inquiry' and the Asset Activity Inquiry will populate.
 - If there are rows returned for the person's User Id and all are acceptable, then the investigation can be concluded.

If you find unauthorized activity and additional research is required to determine what the user may have done, email ELMSSupport@leidos.com to request a help ticket be opened for a Retroactive User Activity Review.

- Provide the User Id for the user being investigated as well as the start and end dates for a date range to be queried.
 - ELMS Support will assign the help ticket to the ELMS Database Team, who will run a database script generating a user activity data report.
 - ELMS Support will send a copy of the report and data files to the IO(s) to support the investigation, and the help ticket will be closed.



For More Information

For more information on the full ELMS system, please visit our ELMS Support site: <https://elmssupport.golearnportal.org>.

For account and user questions, including questions related to IO/AIO appointment and CCB designation, please email ELMSSecurity@leidos.com.

For all other questions, including questions pertaining to training accounts, eLearning support, ELMS login errors, etc., email ELMSSupport@leidos.com or call 1-844-843-3727.

Support Help Desk Email
elmssupport@leidos.com

Call Support Toll Free
1-844-843-3727

ELMS eLearning
<https://elmselearning.golearnportal.org>

ELMS Support Site
<https://elmssupport.golearnportal.org>



Defense Logistics Agency (DLA)
Logistics Catalog and Data Solutions (LCDS)

