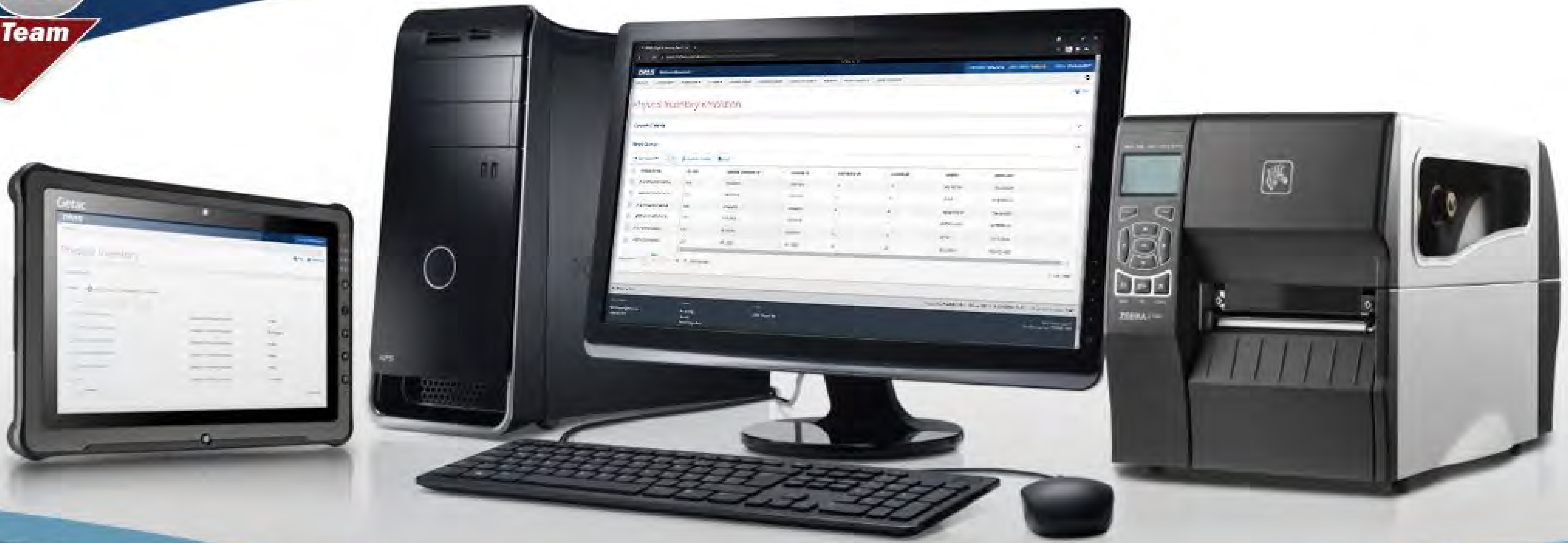
Defense Property Accountability System

DPAS

Support Team



Information Owner & Alternate Information Owner Guide

Office of the Deputy Assistant Secretary of Defense for Logistics
under the Assistant Secretary of Defense for Sustainment

leidos

Table of Contents

Introduction

Congratulations! You have been appointed as a Defense Property Accountability System (DPAS) Information Owner (IO) or Alternate Information Owner (AIO). You are now authorized to sign for DPAS user access requests. The information provided in this packet 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 DPAS Security by emailing DPASSecurity@leidos.com. Any questions regarding training accounts, eLearning support, DPAS log in errors, etc., please contact DPAS Support by emailing DPASSupport@leidos.com or by calling 1-844-843-3727 (1-844-THE-DPAS). Further information on the DPAS system is outlined on our support site: https://dpassupport.golearnportal.org.

Responsibilities of IOs/AIOs

- You are now authorized to sign for user access to the DPAS Tiers you are appointed.
  - You may now 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 DPAS Production account.
- You will verify that roles being assigned to the user do not conflict with other duties or actions in DPAS 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 8.
- You will upload user access request packets, following instructions outlined on pages 6-7.
- You will send a signed email to DPASSecurity@leidos.com confirming when a user no longer requires access, requesting account deletion.
- You will send a signed email to DPASSecurity@leidos.com confirming a user’s new contract information, designation (MIL/CTR/CIV) change, name change, or email change.

Responsibilities of IOs/AIOs

- **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 can be requested by emailing DPASSupport@leidos.com.**
    - **Send a signed email to DPASSecurity@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 DPAS Support requesting a Retroactive User Activity Investigation. Detailed instructions are listed on page 16.**
  - **This occurrence is necessary if a user has access to DPAS longer than required, or if you suspect a user has negatively impacted DPAS data.**
- **You will perform an Annual User Audit each year, initiated when an email is sent by the DPAS Account Management team including instructions and the audit 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).**

DPAS Access Request Instructions

- New user forms are available on our DPAS Support site https://dpassupport.golearnportal.org/.
  - Hover over ‘Support’, select ‘Request Access’, and select the DPAS module the user is requesting access for.
  - Review ‘Download the Forms’, ‘Understand the Forms’, and ‘Submit the Forms’.
  - Select on each user form link, download the form, and save it to your desktop using the required naming convention.
    - All user forms must be named with a consistent naming convention for Account Management and DPAS Auditors to have 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 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) administrator(s).
  - Forms must be saved as PDF files to process successfully once received.
  - Right click on the Folder, hover over ‘Send To’, select ‘Compressed (zipped) Folder’, and name the zip file using the required naming convention.
    - Last Name First Name MI
      - Example: ‘Smith Jane L’
    - Last Name First Name NMN
      - Examples: ‘Smith Jane NMN’

DPAS Access Request Instructions

- A web validation tool can be accessed at https://dpas.dape.dla.mil/new-accounts/
  - Identifies user form corrections necessary before submission.
    - Is not yet programmed to review Roles Request Forms for the FSM, ICP, or Registry modules. Manual review is necessary for these forms.
    - Does not verify the date on the DoD Cyber Awareness Certificate. Manual review is necessary for the certificate.
    - All 2875 date format variations and investigation types may not be included in the web tool's validation. Some formats may still generate an error even though valid. DPAS Security will accept if dates are complete calendar dates and investigation types are valid from Security Manager. DPAS Security can address any questions with the IO/AIO.
  - The tool is for validation purposes only and is not tied to a DPAS account, nor does it load any user information into the system.
  - Allows review of single user forms or a full zipped packet.
    - Drag and drop files into the ‘Drop files here’ box at the top of the screen OR select the magnifying glass to search and select files that need validated.
    - 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 an item needs additional review for form correction.
  - Once user forms are reviewed and validated successfully, you may upload them for processing.
- Visit https://dpaselearning.golearnportal.org/fileupload/useraccess.php to upload a new zipped user packet or individual roles update request.
  - For ‘Request Type’:
    - New Account Creation = ‘Add New User’
    - Update to Existing Account = ‘Update User’
    - ‘Delete User’ is not applicable – account deletion must be a signed email request sent to DPASSecurity@leidos.com.
  - Validation of forms must be complete and accurate for forms to be processed.
    - Use of the web validation tool outlined above assists in avoiding form returns, unnecessary corrections, and required resubmission.
    - If the web validation tool was not utilized prior to form submission, DPAS Security will review and notify the IO to confirm incorrect form completion so that corrections can be made, and forms can be resubmitted.
  - User files received will be downloaded and then removed from the secure upload site.

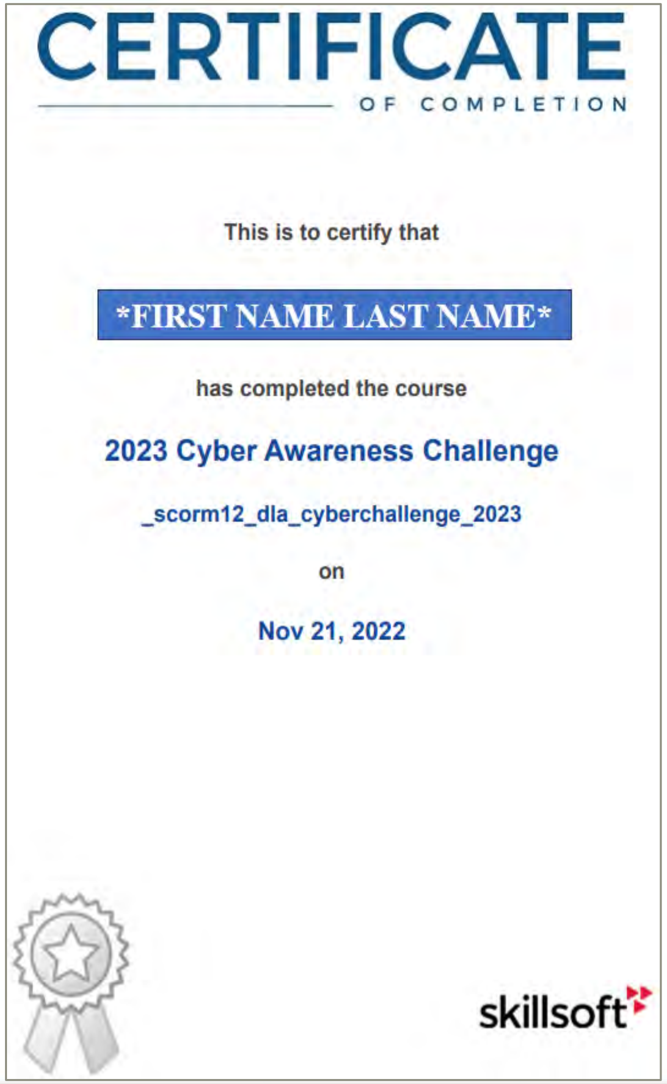
DoD Cyber Awareness Challenge Certificate Requirements

DoD Cyber Awareness Challenge Certificate Requirements

The training certificate must include:

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

An example of the DoD Cyber Awareness Challenge Certificate is provided to the right for your use in comparison.



CERTIFICATE

OF COMPLETION

This is to certify that

FIRST NAME LAST NAME

has completed the course

2023 Cyber Awareness Challenge

_scorm12_dla_cyberchallenge_2023

on

Nov 21, 2022

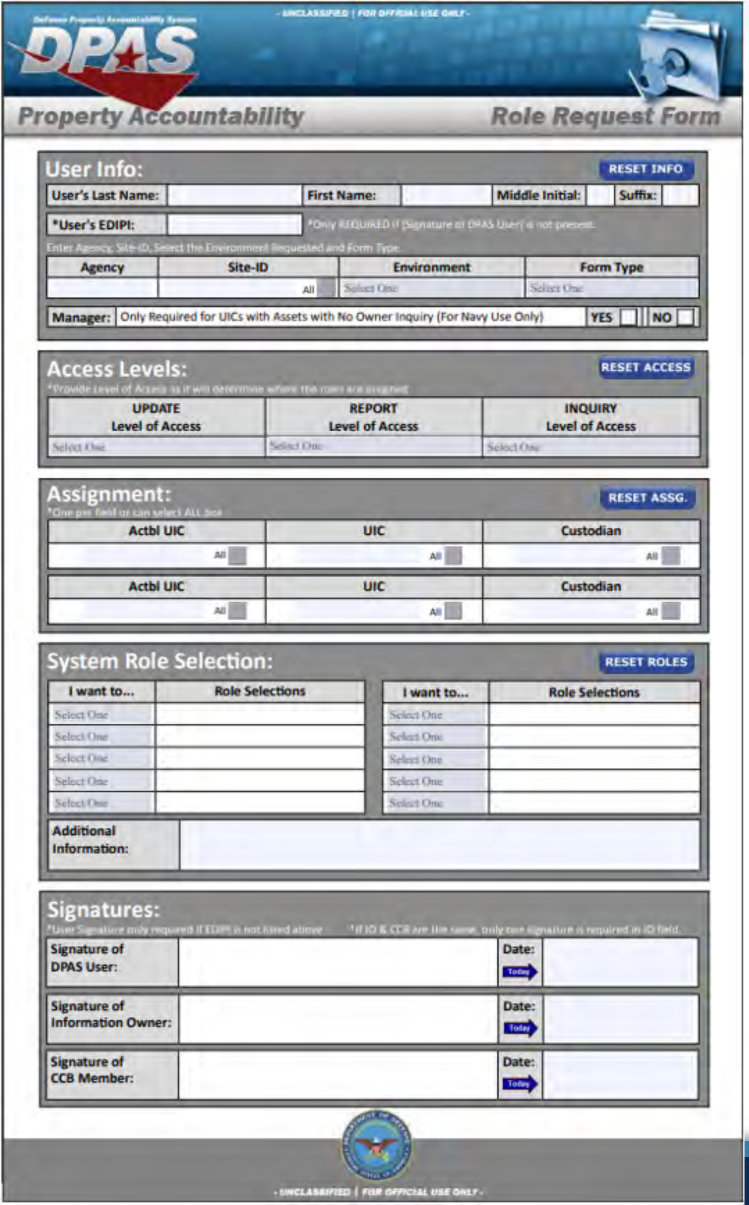
skillsoft

Role Request Form Requirements

- Must be a current form from the DPAS Support Site.
- Used to request new account access or to update existing DPAS access.
  - For updates to existing accounts, complete all necessary fields and note a reason within the 'Additional Information' section.
    - A single form does not need zipped before submission.
- For new access request packets, there must be at least one Role Request form included in submission.
  - Multiple Role Request forms can be included if the user needs access to multiple modules or multiple sites within a module.
- Roles are to be selected per the user's needs.
  - For role descriptions, visit the DPAS Support site, hover over 'System Solutions', hover over 'By Role', and select the module.
  - The IO Role cannot be assigned to a user who hasn't been appointed as an IO.
  - A contractor cannot carry an APO role and must instead request the combination of PA and Catalog Manager roles.
  - The Property Accountability (PA) Role Request Form requires a CCB Signature if the IO signing is not a CCB Member and is requesting an update role at Agency level.
- Access Tier name(s) being requested must already exist within DPAS and be spelled exactly as listed within the system.

An example of the Property Accountability Role Request Form is provided on the next slide.

Role Request Form



User Info:

RESET INFO

User's Last Name:		First Name:		Middle Initial:		Suffix:	
*User's EDIPI:		*Only REQUIRED if (Signature of DPAS User) is not present.					

Enter Agency, Site-ID, Select the Environment Requested and Form Type.

Agency	Site-ID	Environment	Form Type
	All □	Select One	Select One

Manager:	Only Required for UICs with Assets with No Owner Inquiry (For Navy Use Only)	YES □	NO □

Access Levels:

RESET ACCESS

*Provide Level of Access as it will determine where the roles are assigned.

UPDATE Level of Access	REPORT Level of Access	INQUIRY Level of Access
Select One	Select One	Select One

Assignment:

RESET ASSG.

*One per field or can select ALL box

Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	**UIC**	**Custodian**
All □	All □	All □

System Role Selection:

RESET ROLES

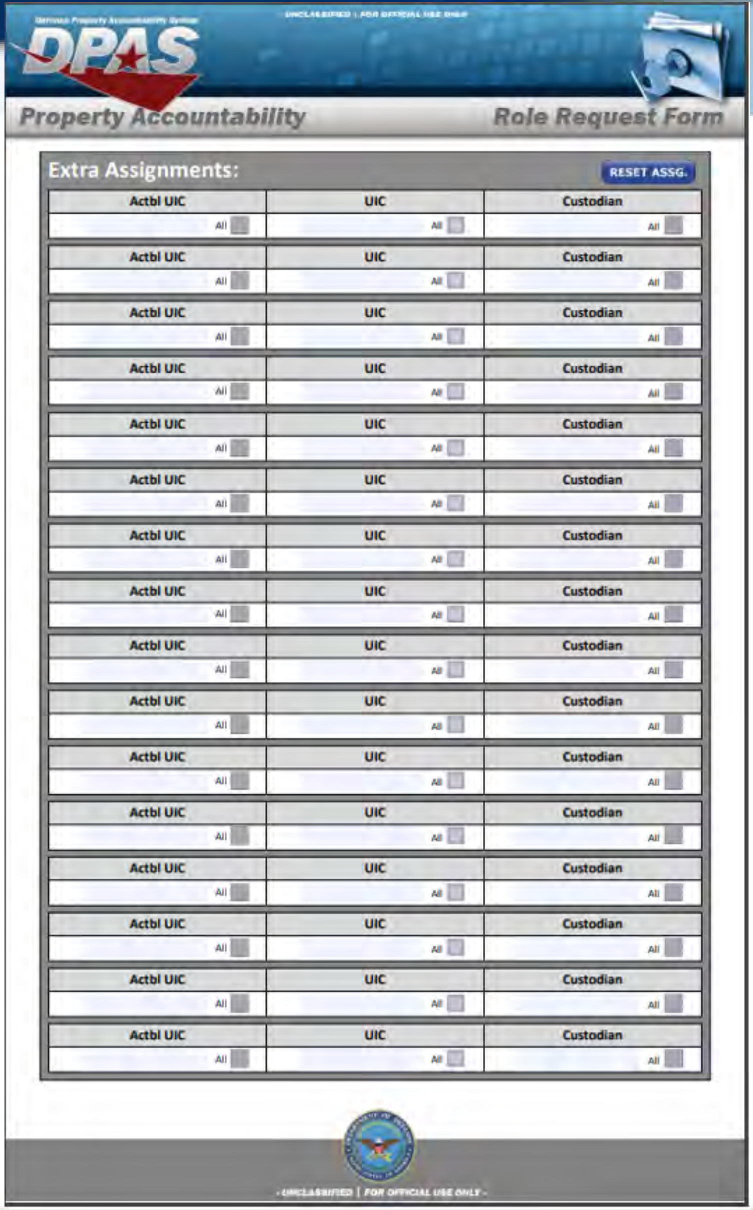
I want to...	Role Selections	I want to...	Role Selections
Select One		Select One	
Select One		Select One	
Select One		Select One	
Select One		Select One	
Select One		Select One	

Additional Information:	

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.

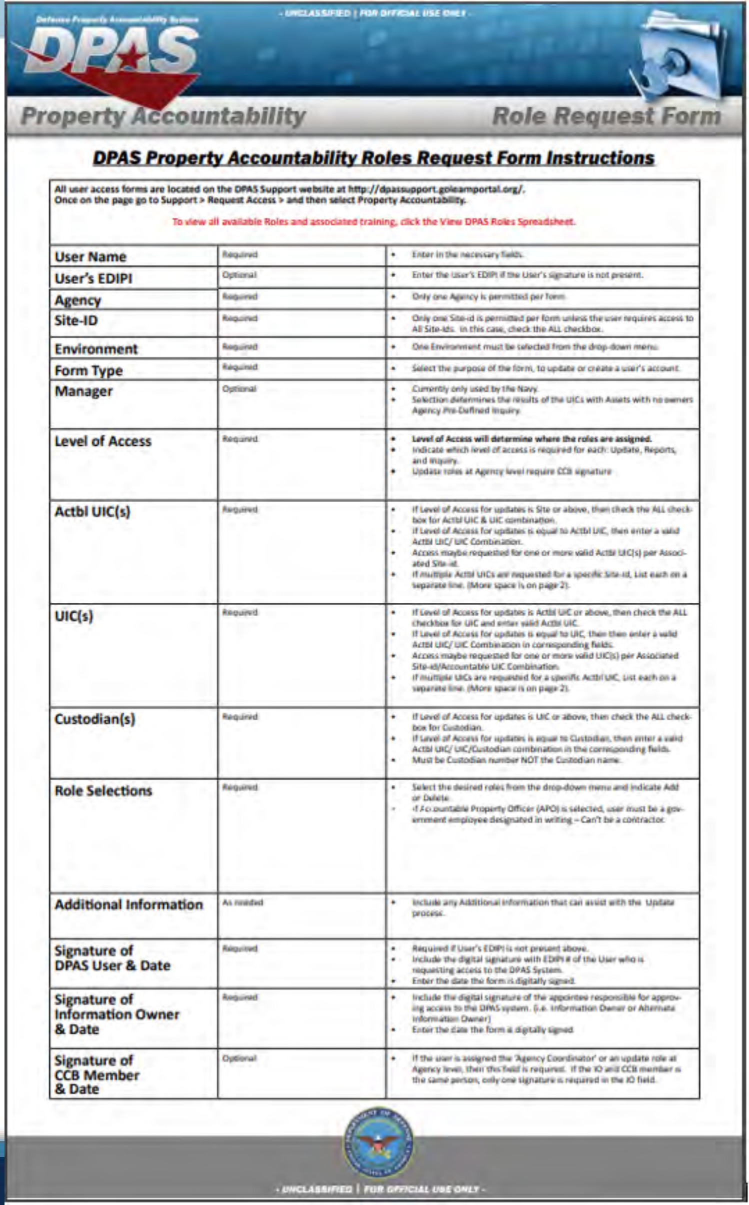
Signature of DPAS User:		Date: Today	
Signature of Information Owner:		Date: Today	
Signature of CCB Member:		Date: Today	



Extra Assignments:

RESET ASSG.

Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □
Actbl UIC	UIC	Custodian
All □	All □	All □



DPAS Property Accountability Roles Request Form Instructions

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

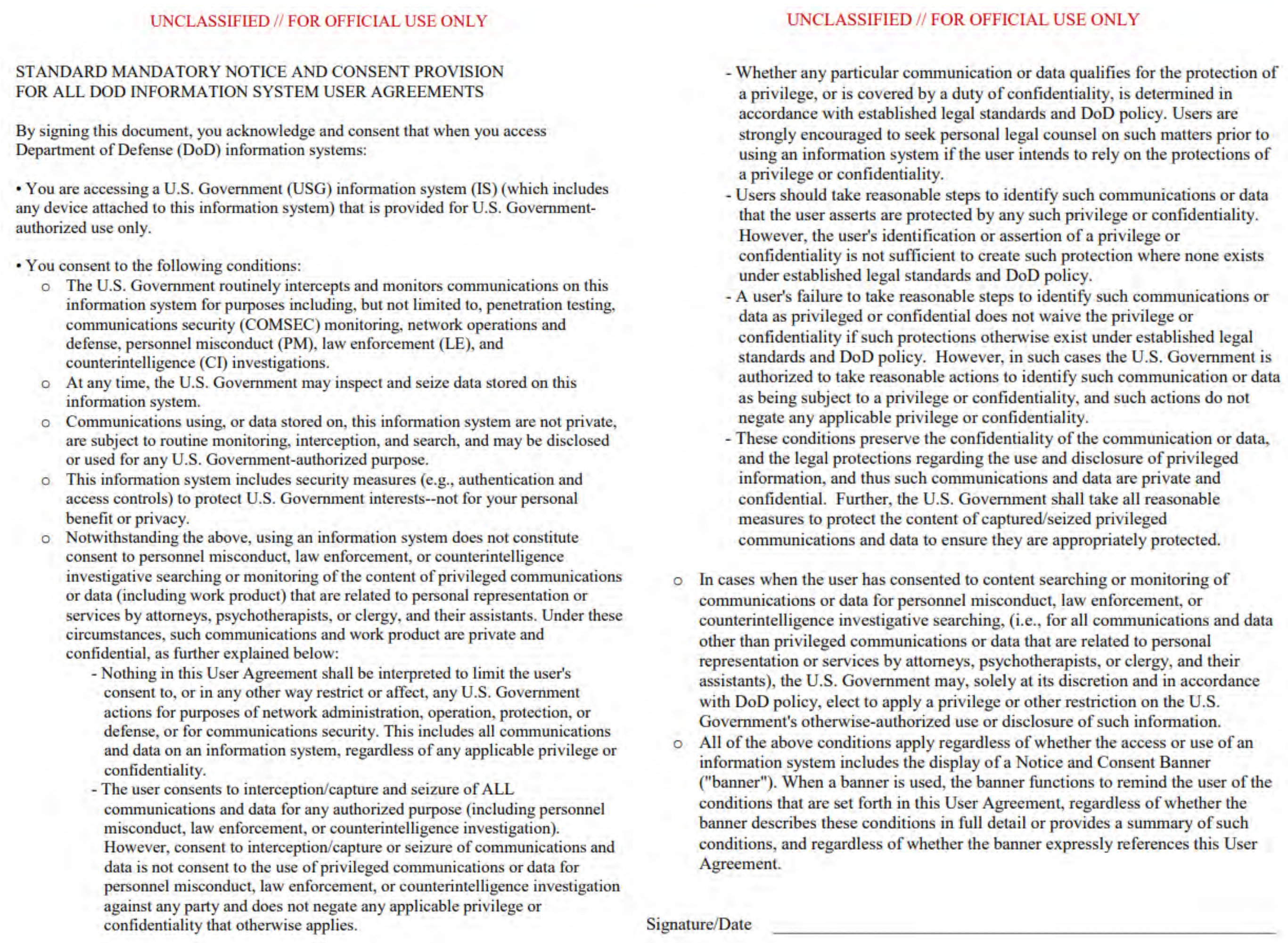
To view all available Roles and associated training, click the View DPAS Roles Spreadsheet.

User Name	Required	• Enter in the necessary fields.
User's EDIPI	Optional	• Enter the User's EDIPI if the User's signature is not present.
Agency	Required	• Only one Agency is permitted per form.
Site-ID	Required	• 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	• One Environment must be selected from the drop-down menu.
Form Type	Required	• Select the purpose of the form, to update or create a user's account.
Manager	Optional	• 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	• **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 CCB signature
Actbl UIC(s)	Required	• 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 maybe 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	• 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 then enter a valid Actbl UIC/ UIC Combination in corresponding fields. • Access maybe 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	• 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	• 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.
Additional Information	As needed	• Include any Additional information that can assist with the Update process.
Signature of DPAS User & Date	Required	• Required if User's EDIPI is not present above. • Include the digital signature with EDIPI # of the User who is requesting access to the DPAS System. • Enter the date the form is digitally signed.
Signature of Information Owner & Date	Required	• Include the digital signature of the appointee responsible for approving access to the DPAS system. (i.e. Information Owner or Alternate Information Owner) • Enter the date the form is digitally signed.
Signature of CCB Member & Date	Optional	• If the user is assigned the 'Agency Coordinator' or an update role at Agency level, then this field is required. If the IO and CCB member is the same person, only one signature is required in the IO field.

User Agreement Form Requirements

User Agreement (UA) Form Requirements

- Must be a current form from the DPAS 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, DPAS Security may approve use of a handwritten signature and handwritten date instead of a digital signature (“wet-signed”).
  - Scanned forms are not acceptable and will be returned.



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

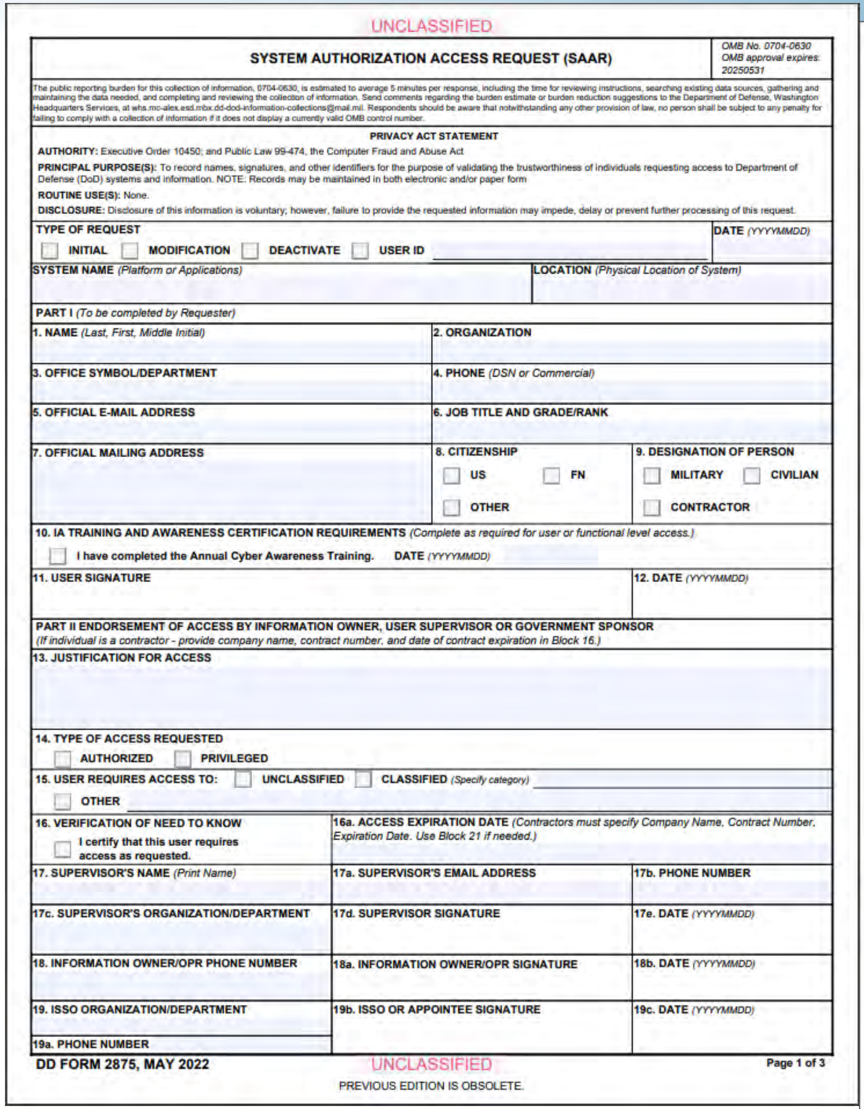
  - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using 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 ______________________________

SAAR-DD2875 Form Requirements

SAAR-DD2875 Form Requirements

- Must be a current form from the DPAS Support Site.
- Forms that have been altered and will not process, will be returned.
- Digital Signatures must be completed using a federally issued PKI cert and must have the EDIPI present within the signature.
- Digital Signatures must be dated within the past year.
- Signature order by date/time stamp (<u>time zones must be considered</u>):
  - 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 = DPAS
  - 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 the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.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
□ INITIAL □ MODIFICATION □ DEACTIVATE □ USER ID
DATE *(YYYYMMDD)*

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
□ US □ FN
□ OTHER
9. DESIGNATION OF PERSON
□ MILITARY □ CIVILIAN
□ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
□ 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
□ AUTHORIZED □ PRIVILEGED

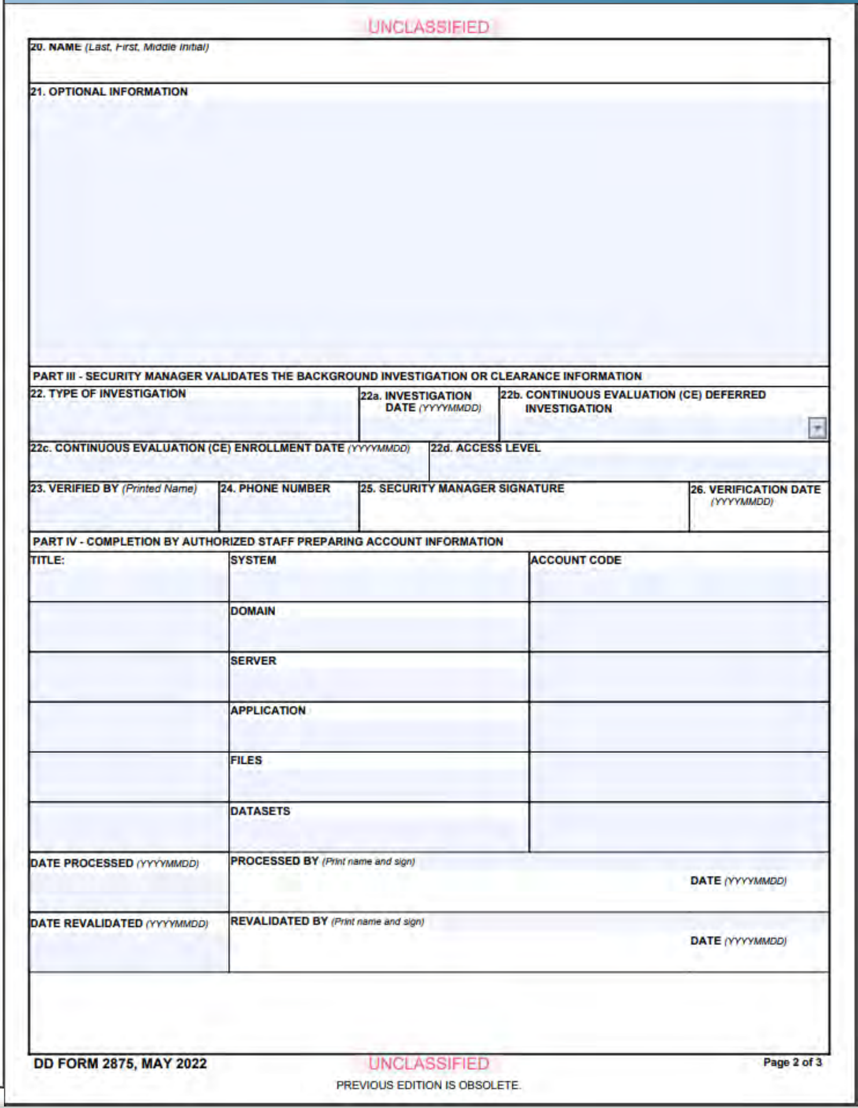
15. USER REQUIRES ACCESS TO: □ UNCLASSIFIED □ CLASSIFIED *(Specify category)*
□ OTHER

16. VERIFICATION OF NEED TO KNOW
□ 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

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



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)*

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

SAAR-DD2875 Form Breakdown

- Part I – User Section
  - Boxes 1-11 must be completed
    - 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 completed
    - Box 14 = Authorized and Box 15 = Unclassified
    - Box 16 must be checked
    - Box 16a needs completed for CONTRACTORS 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 completed by User and Supervisor to ensure data is complete and accurate.
  - Boxes 22-25 must be completed
    - A user must have an investigation completed or at the very least initiated.
    - If a user does not have a Clearance Level, ‘NONE’ can be listed for box 22c.
- IO/AIO Section
  - The IO/AIO will review to make sure all prior sections have been completed in the correct order.
  - The IO/AIO will complete boxes 18 and 18a.
  - The IO/AIO is the last digital signature on the form to authorize account creation before uploading the new user packet request for processing.
- DPAS Account Management Section
  - Boxes 19-19b are reserved for DPAS Account Management completion.
    - The DPAS Security Officer will complete boxes 19-19b once the user packet is ready for account request processing and account generation.
      - <u>If Boxes 19-19b are not left blank for Security Officer completion, the user account request packet will be returned</u>.

Common Reasons for User Access Request Packet Return

- 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 within a year.
- Incomplete or incorrect form fields on one or all forms.
    - The ‘System Name’ is not listed as ‘DPAS’ 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 verified on the SAAR-DD2875.
    - The access tier requested on the Roles Request Form does not match the tier name within DPAS.
    - 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.
    - 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 SOD.
    - Digital signature error on any of the forms.
        - In rare cases, DPAS Security may approve use of a handwritten signature on the UA instead of a digital signature. In these cases, the form date must also be handwritten.

IO Retroactive User Activity Investigation Description

If an IO/AIO identifies a user who had access to DPAS and did not require it, or negative impact to DPAS 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.

IO Retroactive User Activity Investigation Steps

The IO will start the investigation by running a DPAS Accounting Transaction Inquiry and review to verify if the user under investigation conducted any questionable actions.

- Log into the 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 >= 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 they are acceptable, then you can conclude the investigation.
  - If you find unauthorized activity and additional research is required to determine what the user may have done, send a digitally signed email to DPASSecurity@leidos.com requesting immediate user access removal.

If any unauthorized activity is identified within the DPAS Accounting Transaction Inquiry, the IO will run a DPAS Asset Activity Inquiry and review to determine if the user conducted further questionable actions.

- Log into the PA module, hover over ‘Inquiries’, hover over ‘Asset Management’, and select ‘Asset Activity’.
- Enter a Transaction Dt 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 they are acceptable, then you can conclude the investigation.
  - If you find unauthorized activity and additional research is required to determine what the user may have done, email DPASSupport@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.
      - DPAS Support will assign the help ticket to the DPAS Database Team, who will run a database script generating a user activity data report.
      - DPAS 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.

IOs are responsible for investigating user activities to determine insider threats, reporting to the appropriate authority, and resolving any impacts to financial records that are applicable.

Questions

For further information on the full DPAS system, please visit our DPAS Support site: https://dpassupport.golearnportal.org.

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

For all other questions, including questions pertaining to training accounts, eLearning support, DPAS login errors, etc., email DPASSupport@leidos.com or call 1-844-THE-DPAS (1-844-843-3727).