INSTRUCTIONS TO REGISTER AND ACCESS THE IDENTITY MANAGEMENT (IDM) AND ENTERPRISE PORTAL WEBSITE AND ADD ENTERPRISE BASIC ACCESS

HTTPS://IDM.AESIP.ARMY.MIL

HTTPS://WWW.AESIP.ARMY.MIL/IRJ/PORTAL

HTTPS://IDM.AESIP.ARMY.MIL
THE WEBSITE WORKS BEST ON CHROME

- Currently IDM is available across a DoD network or VPN connection. Coordination is in progress to allow access from non-DoD networks.
- New users will need to register in the AESIP Hub Enterprise IDM and update profile information, to include their Supervisor and Security Officer, prior to submitting any new requests.
- Use the magnifying glass next to the Supervisor field and select “reassign” link to search. The * can be used as a wild card when searching. There could be several John Smith entries, so check the “Email” to make sure you are selecting the correct Security Officer. **TIP** When searching for the Security Officer choose First name or Last name to search by.

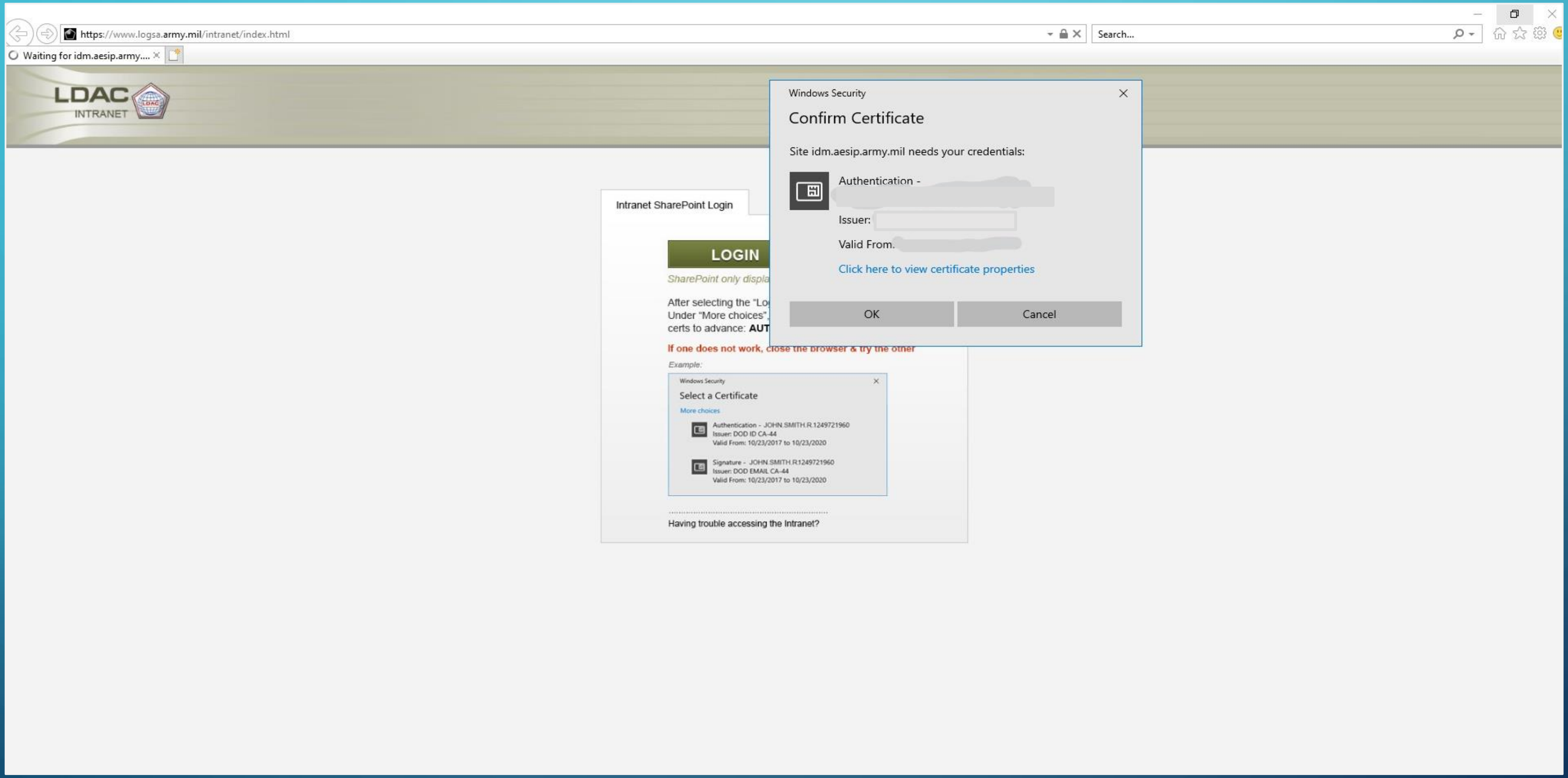
SUPERVISORS AND SECURITY OFFICERS

- Supervisors and Security Managers (SM) / Facilities Security Officers (FSO) must be registered in IDM prior to users selecting them.
- Supervisors and Security Managers can NOT be the same person
- You can not put yourself as your own Supervisor or Security Manager; any roles you put in will be rejected if you do this
- SM / FSO do not need to update their profile information, but they do need to register.
- If your supervisor or SM/FSO needs help on registering, please refer to page 7 of this PowerPoint. If you need more information, please refer to the contact information at the end of this PowerPoint.

INSTRUCTIONS FOR LOGGING INTO BOTH WEBSITES

- https://login.aesip.army.mil (ONLY to Register)
- https://idm.aesip.army.mil (Identity Management)
- https://www.aesip.army.mil/irj/portal (AESIP Enterprise Portal)

WHEN YOU ARE PROMPTED FOR A CERTIFICATE, CHOOSE AUTHENTICATION



https://www.logsa.army.mil/intranet/index.html

Waiting for idm.aesip.army....

Intranet SharePoint Login

LOGIN

SharePoint only displa

After selecting the "Lo
Under "More choices",
certs to advance: **AUT**

If one does not work, close the browser & try the other

Example:

Windows Security

Select a Certificate

More choices

Authentication - JOHN.SMITH.R.1249721960
Issuer: DOD ID CA-44
Valid From: 10/23/2017 to 10/23/2020

Signature - JOHN.SMITH.R.1249721960
Issuer: DOD EMAIL CA-44
Valid From: 10/23/2017 to 10/23/2020

Having trouble accessing the Intranet?

Windows Security

Confirm Certificate

Site idm.aesip.army.mil needs your credentials:

Authentication - [redacted]

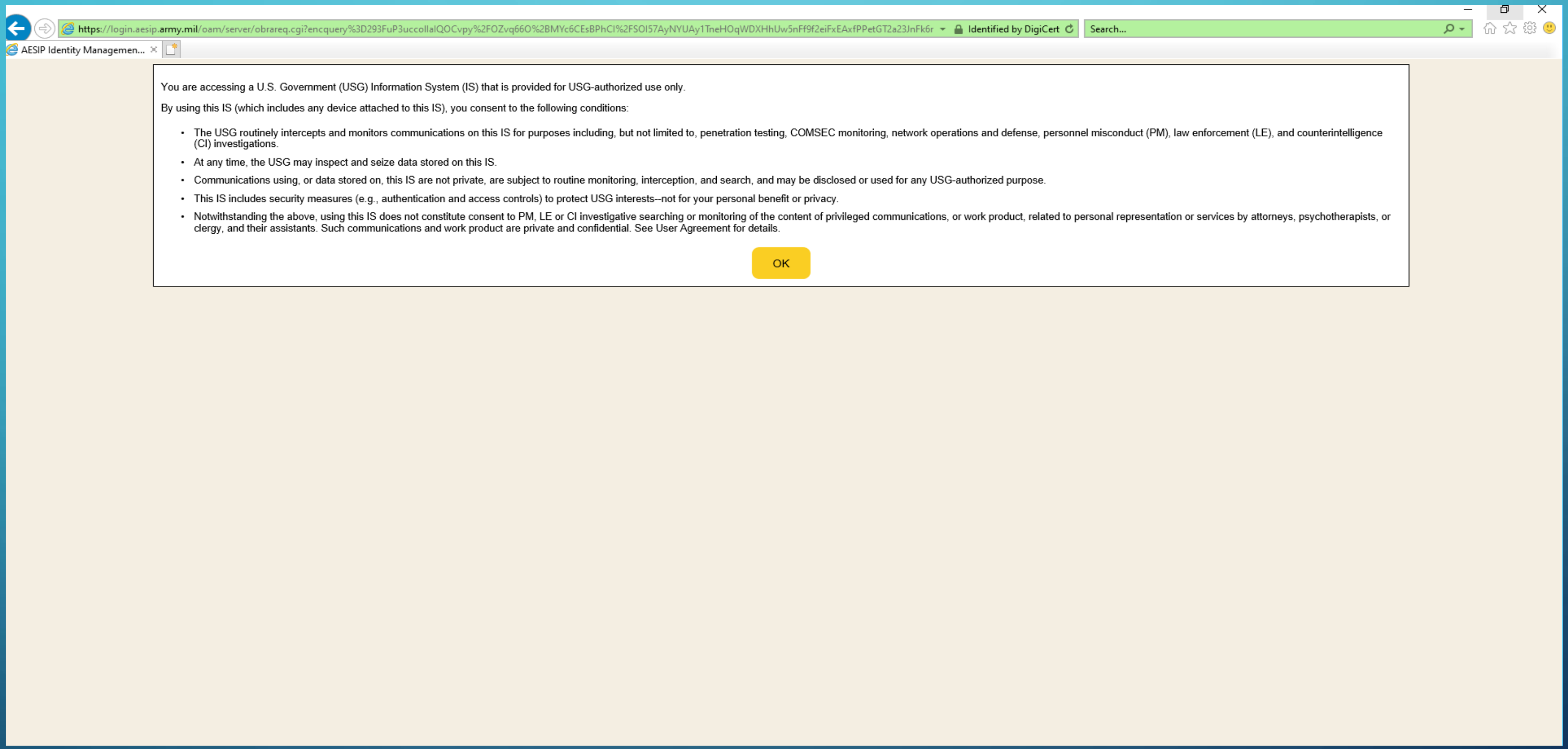
Issuer: [redacted]

Valid From. [redacted]

Click here to view certificate properties

OK | Cancel

CLICK OK



https://login.aesip.army.mil/oam/server/obrareq.cgi?encquery%3D293FuP3uccollalQOCvpy%2FOZvq66O%2BMYc6CEsBPhCI%2FSOI57AyNYUAy1TneHOqWDXHhUw5nFf9f2eiFxEAxfPPetGT2a23JnFk6r
Identified by DigiCert
Search...
AESIP Identity Managemen...

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

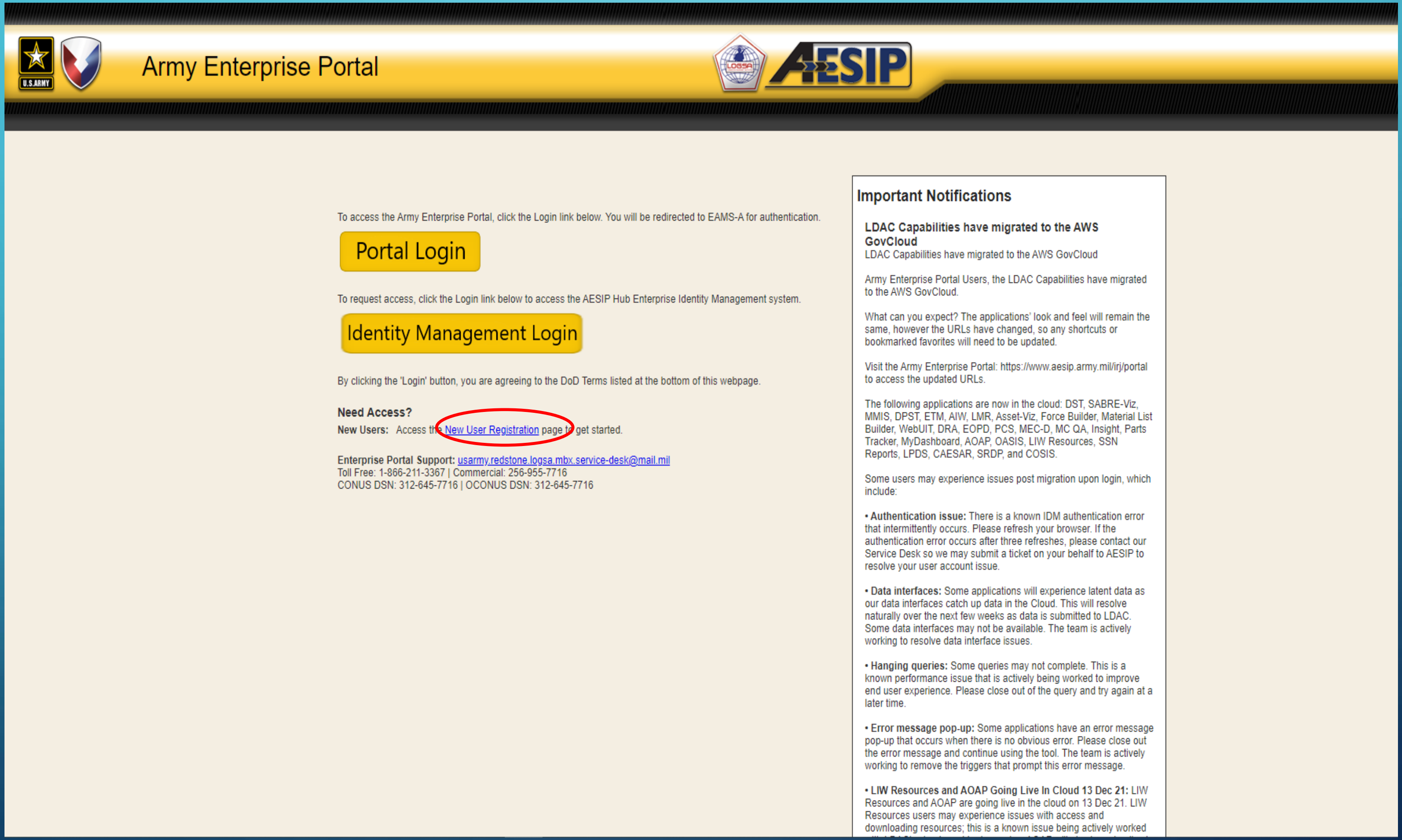
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

REGISTERING FOR AN AESIP ACCOUNT

- Go to https://login.aesip.army.mil
- Click the link under the “Need Access?” section. *DO NOT SELECT EXTERNAL APPROVER*
- Use your 16-digit Authentication Certificate (PIV) when prompted.
- This will complete the registration with a “Successful” message and an email will be sent out.
- To login to the IDM navigate to https://idm.aesip.army.mil

REGISTERING A NEW ACCOUNT



To access the Army Enterprise Portal, click the Login link below. You will be redirected to EAMS-A for authentication.

To request access, click the Login link below to access the AESIP Hub Enterprise Identity Management system.

By clicking the 'Login' button, you are agreeing to the DoD Terms listed at the bottom of this webpage.

Need Access?

New Users: Access the New User Registration page to get started.

Enterprise Portal Support: usarmy.redstone.logsa.mbx.service-desk@mail.mil
Toll Free: 1-866-211-3367 | Commercial: 256-955-7716
CONUS DSN: 312-645-7716 | OCONUS DSN: 312-645-7716

Important Notifications

LDAC Capabilities have migrated to the AWS GovCloud
LDAC Capabilities have migrated to the AWS GovCloud

Army Enterprise Portal Users, the LDAC Capabilities have migrated to the AWS GovCloud.

What can you expect? The applications' look and feel will remain the same, however the URLs have changed, so any shortcuts or bookmarked favorites will need to be updated.

Visit the Army Enterprise Portal: https://www.aesip.army.mil/irj/portal to access the updated URLs.

The following applications are now in the cloud: DST, SABRE-Viz, MMIS, DPST, ETM, AIW, LMR, Asset-Viz, Force Builder, Material List Builder, WebUIT, DRA, EOPD, PCS, MEC-D, MC QA, Insight, Parts Tracker, MyDashboard, AOAP, OASIS, LIW Resources, SSN Reports, LPDS, CAESAR, SRDP, and COSIS.

Some users may experience issues post migration upon login, which include:

• **Authentication issue:** There is a known IDM authentication error that intermittently occurs. Please refresh your browser. If the authentication error occurs after three refreshes, please contact our Service Desk so we may submit a ticket on your behalf to AESIP to resolve your user account issue.

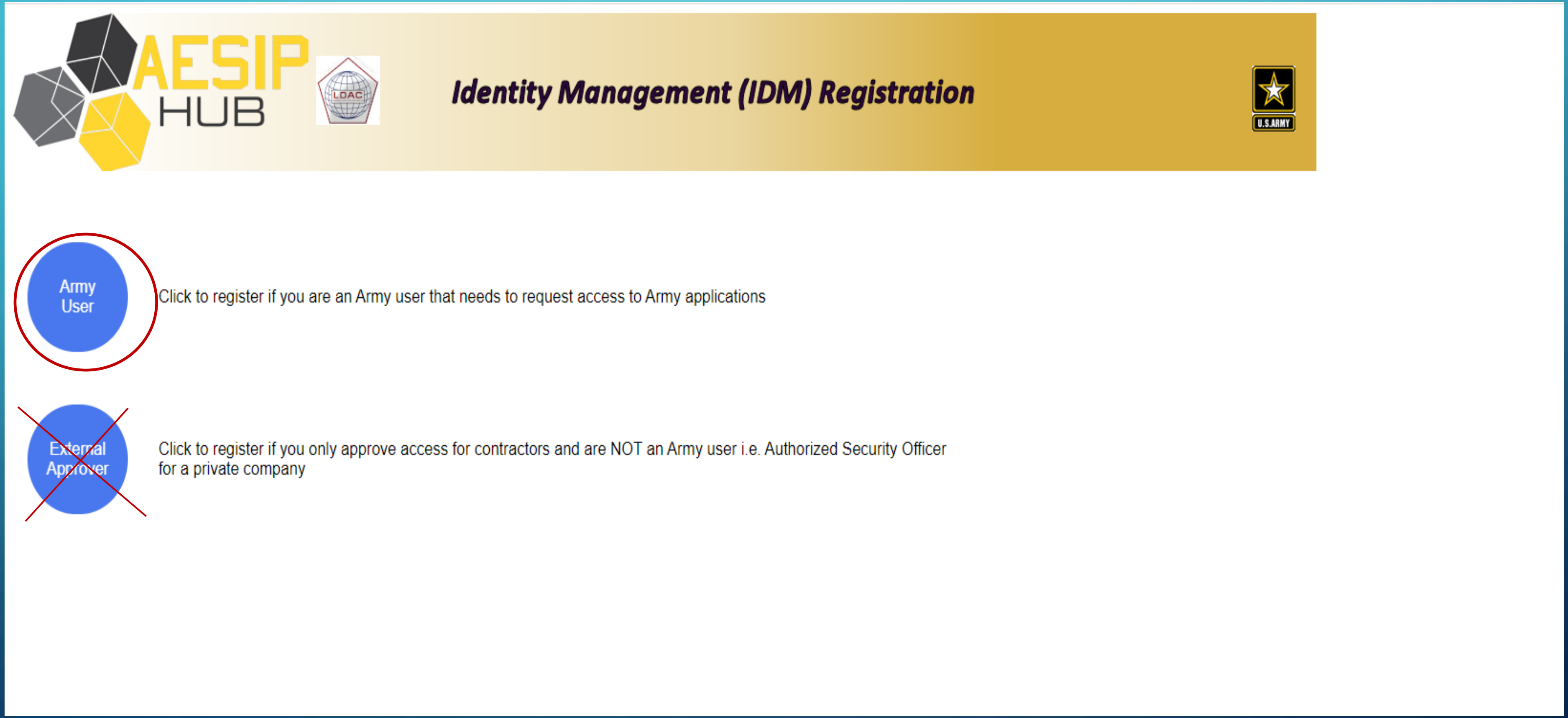
• **Data interfaces:** Some applications will experience latent data as our data interfaces catch up data in the Cloud. This will resolve naturally over the next few weeks as data is submitted to LDAC. Some data interfaces may not be available. The team is actively working to resolve data interface issues.

• **Hanging queries:** Some queries may not complete. This is a known performance issue that is actively being worked to improve end user experience. Please close out of the query and try again at a later time.

• **Error message pop-up:** Some applications have an error message pop-up that occurs when there is no obvious error. Please close out the error message and continue using the tool. The team is actively working to remove the triggers that prompt this error message.

• **LIW Resources and AOAP Going Live In Cloud 13 Dec 21:** LIW Resources and AOAP are going live in the cloud on 13 Dec 21. LIW Resources users may experience issues with access and downloading resources; this is a known issue being actively worked

DO NOT CHOOSE EXTERNAL APPROVER

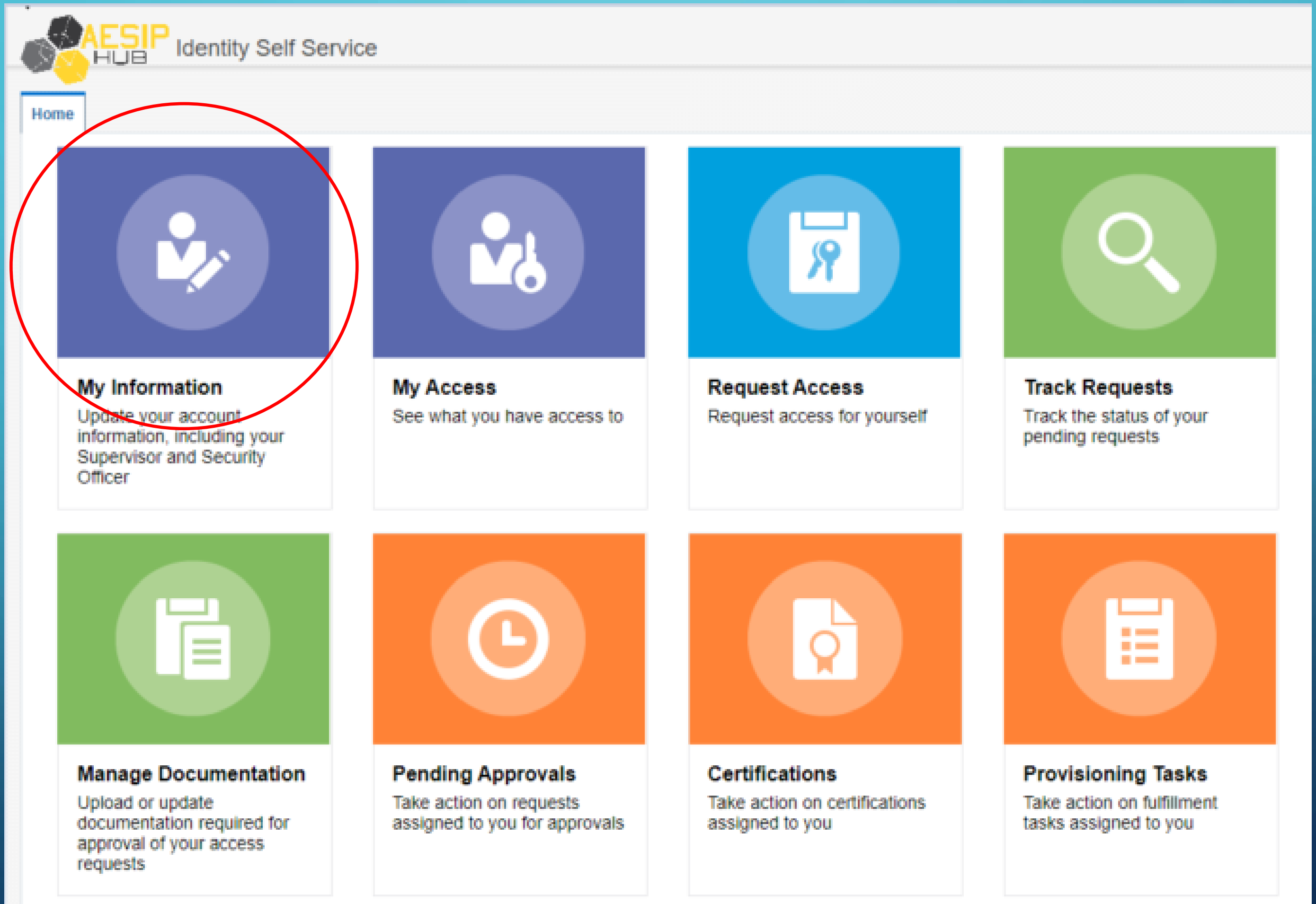


Identity Management (IDM) Registration

Click to register if you are an Army user that needs to request access to Army applications

Click to register if you only approve access for contractors and are NOT an Army user i.e. Authorized Security Officer for a private company

THIS IS THE IDM (IDENTITY MANAGEMENT) HOME PAGE, CHOOSE THE TOP LEFT BLOCK – MY INFORMATION.



AESIP HUB Identity Self Service

Home

My Information
Update your account information, including your Supervisor and Security Officer

My Access
See what you have access to

Request Access
Request access for yourself

Track Requests
Track the status of your pending requests

Manage Documentation
Upload or update documentation required for approval of your access requests

Pending Approvals
Take action on requests assigned to you for approvals

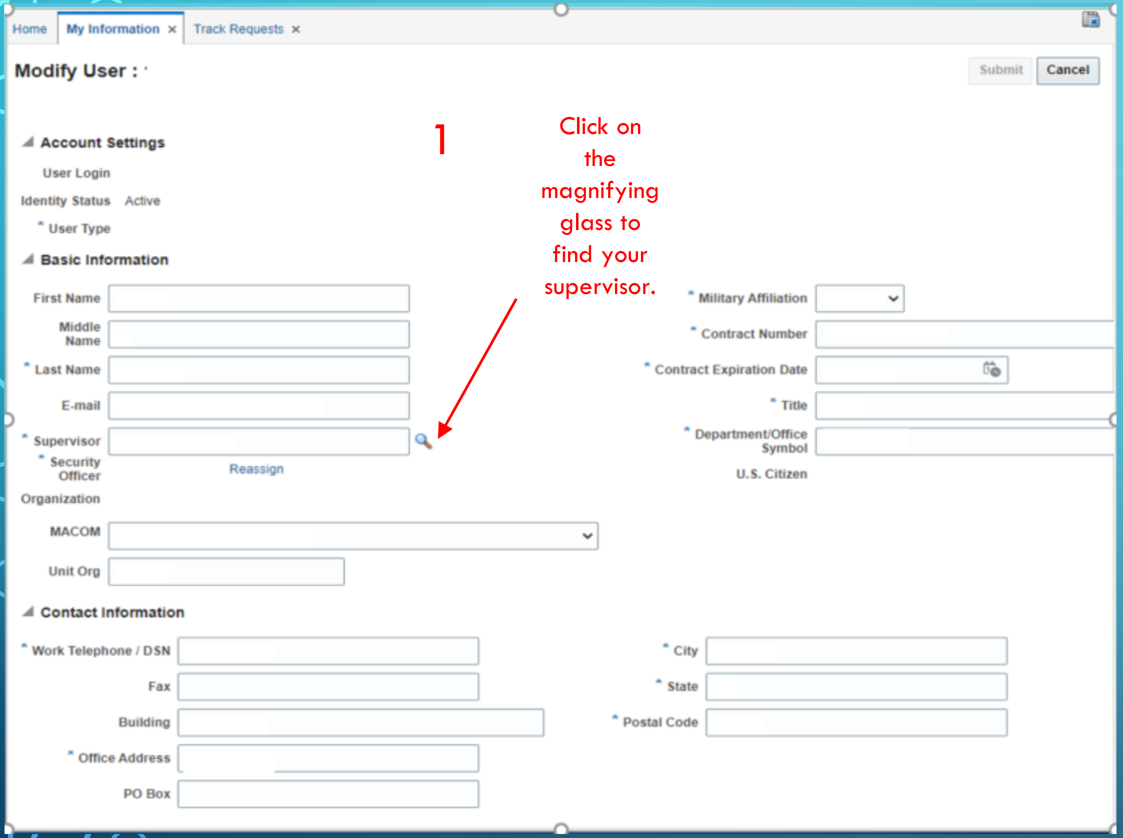
Certifications
Take action on certifications assigned to you

Provisioning Tasks
Take action on fulfillment tasks assigned to you

Update all your personal information.

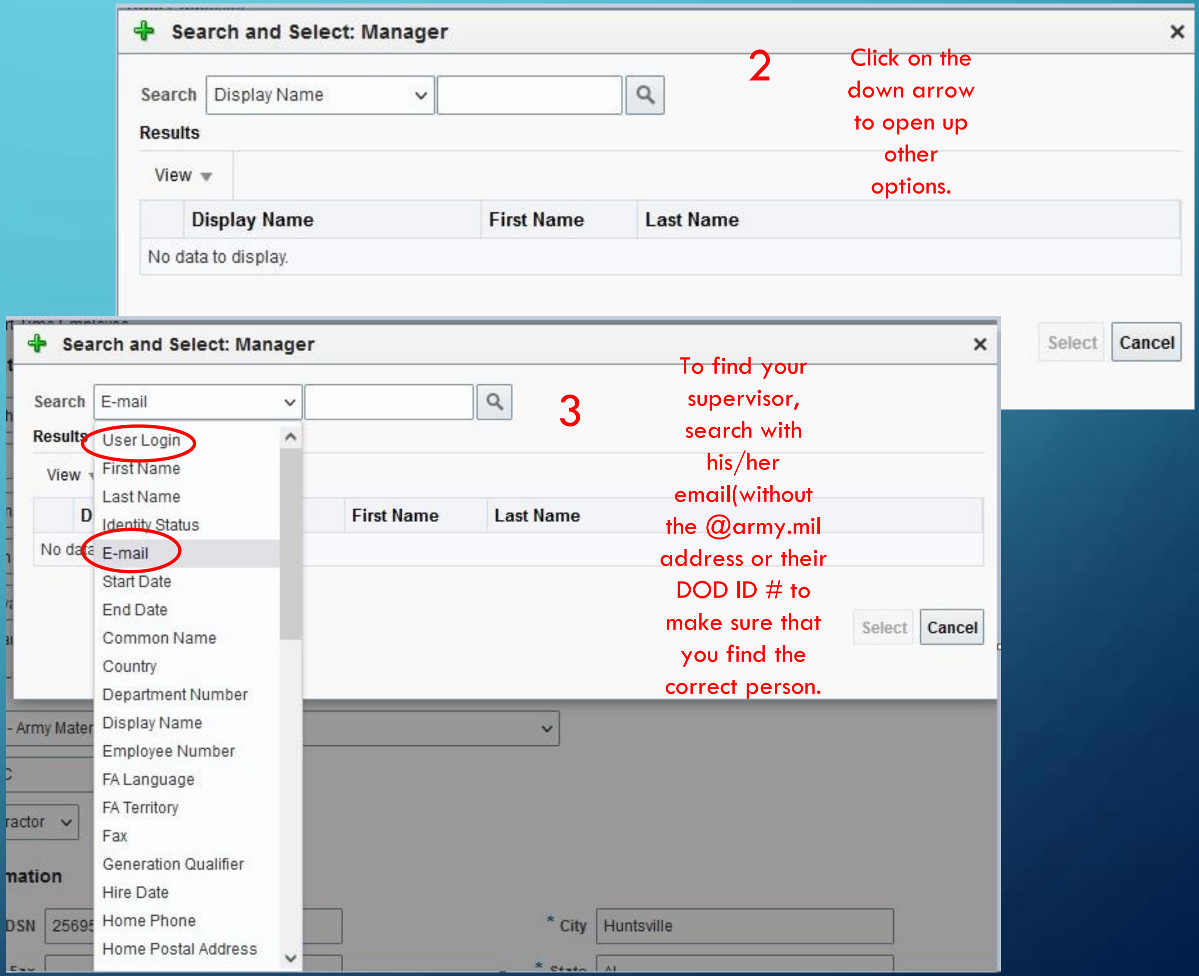
- Supervisors and Security Managers (SM)/Facilities Security Officers (FSO) **must** be registered in IDM prior to users selecting them. If they do not have an Aesip account, send them the short registration instructions at the very end of this PowerPoint.
- Make sure that your Supervisor's email address is correct.
- SM/FSO do not need to update their profile information, but they do need to register.
- Also, the supervisor and S.O. can't be the same person.

FINDING YOUR SUPERVISOR



Identity Status Active

1 Click on the magnifying glass to find your supervisor.



Search Display Name

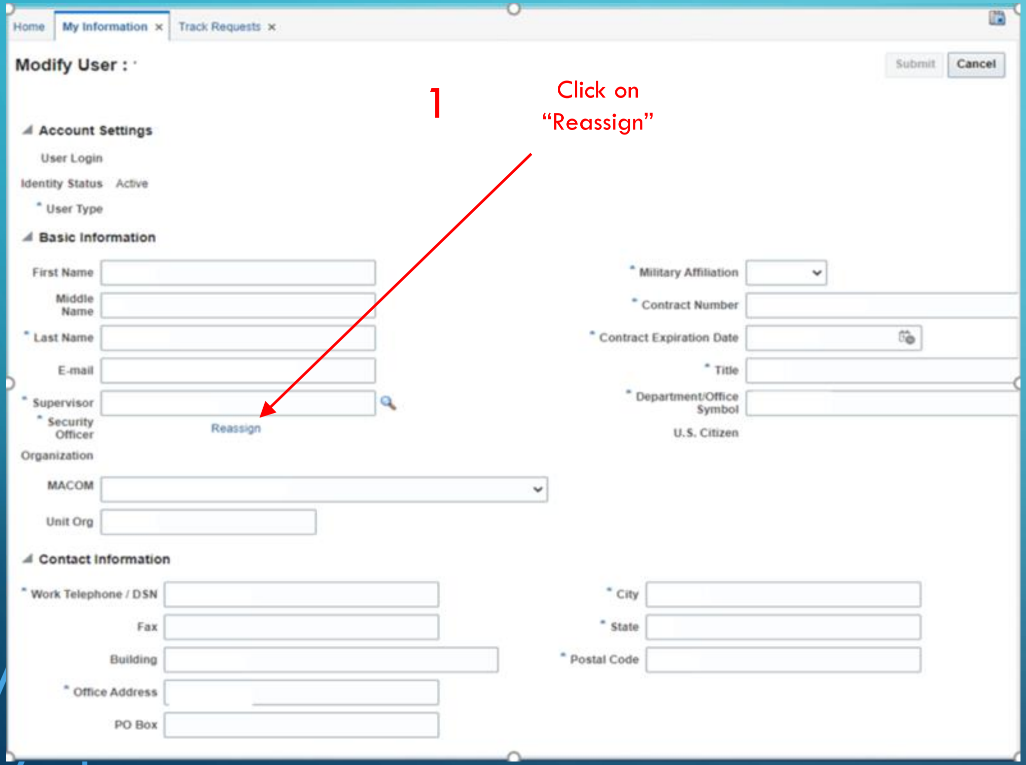
Search E-mail

City Huntsville

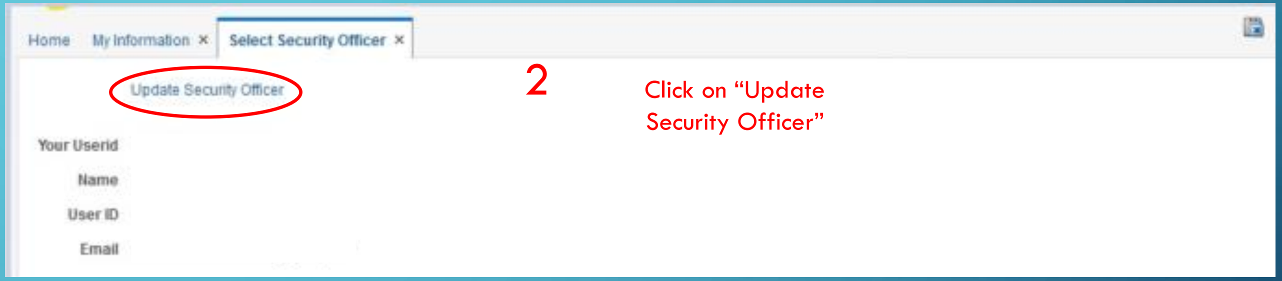
2 Click on the down arrow to open up other options.

3 To find your supervisor, search with his/her email(without the @army.mil address or their DOD ID # to make sure that you find the correct person.

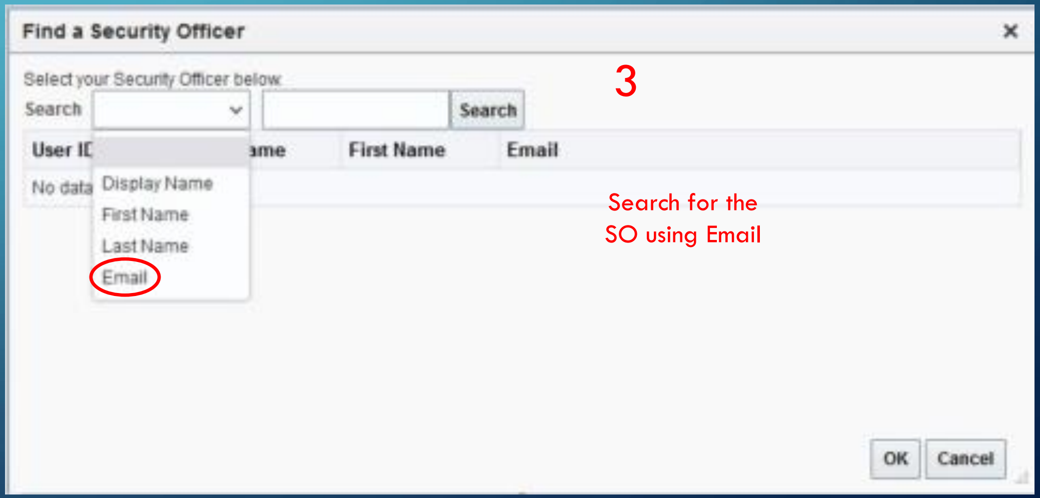
FINDING YOUR SECURITY OFFICER



1 Click on "Reassign"

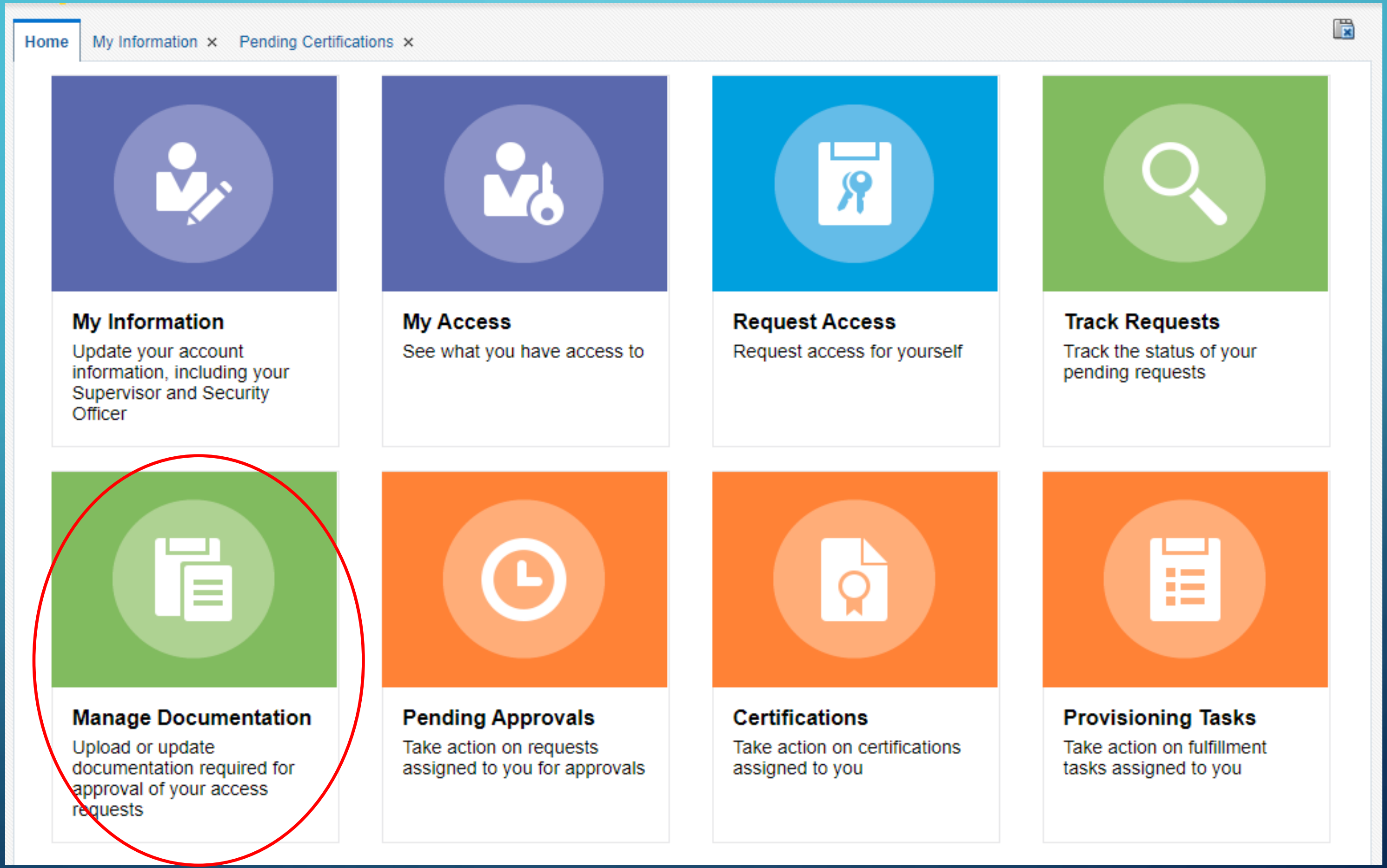


2 Click on "Update Security Officer"



3 Search for the SO using Email

AFTER UPDATING YOUR INFORMATION, GO BACK TO THE HOME PAGE CLICK ON MANAGE DOCUMENTATION



My Information
Update your account information, including your Supervisor and Security Officer

My Access
See what you have access to

Request Access
Request access for yourself

Track Requests
Track the status of your pending requests

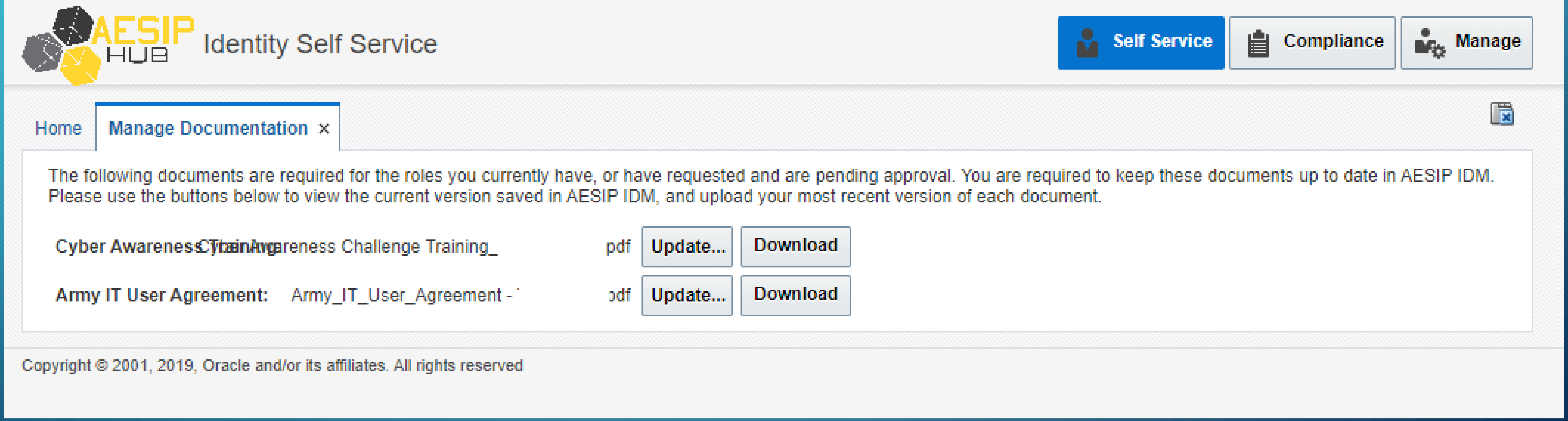
Manage Documentation
Upload or update documentation required for approval of your access requests

Pending Approvals
Take action on requests assigned to you for approvals

Certifications
Take action on certifications assigned to you

Provisioning Tasks
Take action on fulfillment tasks assigned to you

DOWNLOAD CYBER AWARENESS AND ARMY IT USER AGREEMENT DOCUMENTS



The following documents are required for the roles you currently have, or have requested and are pending approval. You are required to keep these documents up to date in AESIP IDM. Please use the buttons below to view the current version saved in AESIP IDM, and upload your most recent version of each document.

Cyber Awareness Training:	Cyber Awareness Challenge Training_	pdf	Update...	Download
Army IT User Agreement:	Army_IT_User_Agreement -	pdf	Update...	Download

Copyright © 2001, 2019, Oracle and/or its affiliates. All rights reserved

ARMY IT USER AGREEMENT

1) Go to the website https://cs.signal.army.mil

2) Click on "LOGIN" at the top of the screen

3) Select Log in with CAC DoD-Approved Certificate Login

4) Under Cyber Security User Portal - Select the following -Select a Branch: Army -Select a Type: Select your affiliation (Civilian, Contractor, or Military) -Select a MACOM: USAASC U.S. Army Acquisition Support Center Click confirm

5) Click on "Sign AUP"

6) Read and at the bottom of the page, click on (Click to digitally sign)

7) When finished click the "CLICK HERE" button at the top of the screen

8) Next click View AUP button. This will display the AUP including your CAC signature at the bottom.

9) Hold down the CTRL key on your keyboard and press P. If successful it will bring up the printer options.

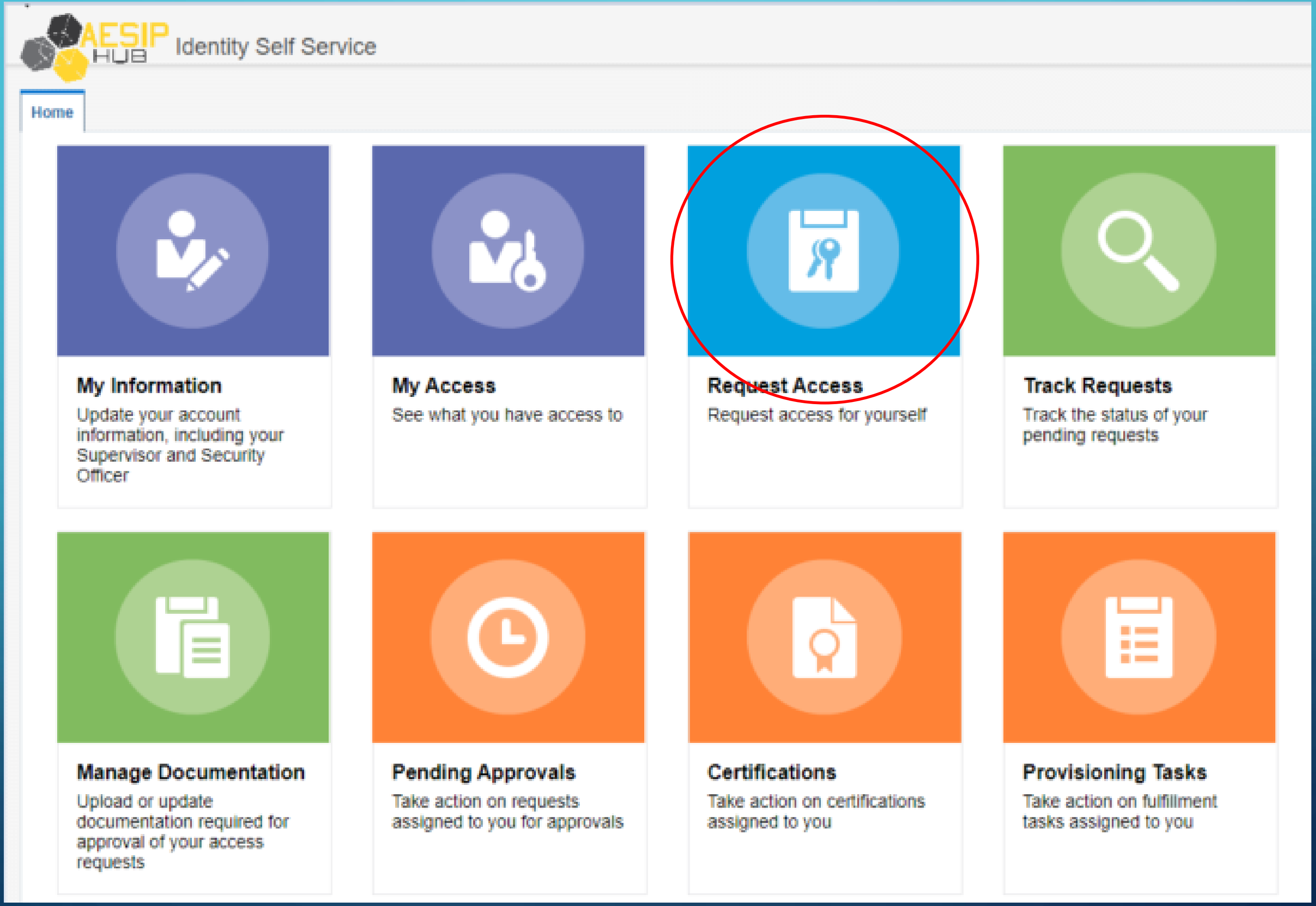
10) Select Adobe PDF from the Select Printer menu

11) Click Print

12) Choose the location to save the file and click Save.

13) You must close the screen to exit

GO BACK TO THE HOME PAGE. CHOOSE REQUEST ACCESS



My Information
Update your account information, including your Supervisor and Security Officer

My Access
See what you have access to

Request Access
Request access for yourself

Track Requests
Track the status of your pending requests

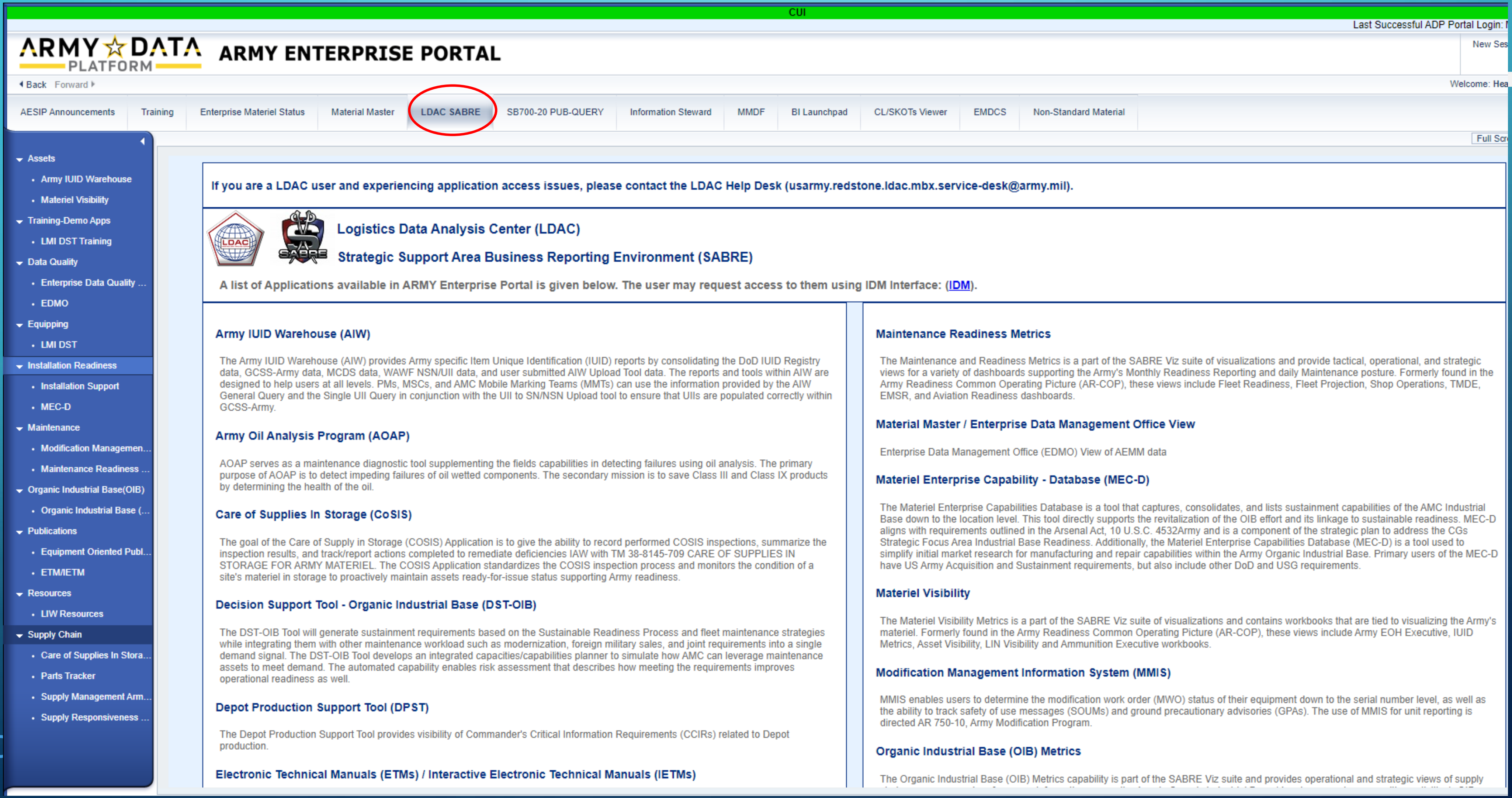
Manage Documentation
Upload or update documentation required for approval of your access requests

Pending Approvals
Take action on requests assigned to you for approvals

Certifications
Take action on certifications assigned to you

Provisioning Tasks
Take action on fulfillment tasks assigned to you

THE ENTERPRISE BASIC ROLE WILL GIVE YOU THE LDAC SABRE TAB IN THE AESIP ENTERPRISE PORTAL



If you are a LDAC user and experiencing application access issues, please contact the LDAC Help Desk (usarmy.redstone.ldac.mbx.service-desk@army.mil).

Logistics Data Analysis Center (LDAC)

Strategic Support Area Business Reporting Environment (SABRE)

A list of Applications available in ARMY Enterprise Portal is given below. The user may request access to them using IDM Interface: (IDM).

Army IUID Warehouse (AIW)

The Army IUID Warehouse (AIW) provides Army specific Item Unique Identification (IUID) reports by consolidating the DoD IUID Registry data, GCSS-Army data, MCDS data, WAWF NSN/UII data, and user submitted AIW Upload Tool data. The reports and tools within AIW are designed to help users at all levels. PMs, MSCs, and AMC Mobile Marking Teams (MMTs) can use the information provided by the AIW General Query and the Single UII Query in conjunction with the UII to SN/NSN Upload tool to ensure that UIIs are populated correctly within GCSS-Army.

Army Oil Analysis Program (AOAP)

AOAP serves as a maintenance diagnostic tool supplementing the fields capabilities in detecting failures using oil analysis. The primary purpose of AOAP is to detect impeding failures of oil wetted components. The secondary mission is to save Class III and Class IX products by determining the health of the oil.

Care of Supplies In Storage (CoSIS)

The goal of the Care of Supply in Storage (COSIS) Application is to give the ability to record performed COSIS inspections, summarize the inspection results, and track/report actions completed to remediate deficiencies IAW with TM 38-8145-709 CARE OF SUPPLIES IN STORAGE FOR ARMY MATERIEL. The COSIS Application standardizes the COSIS inspection process and monitors the condition of a site's materiel in storage to proactively maintain assets ready-for-issue status supporting Army readiness.

Decision Support Tool - Organic Industrial Base (DST-OIB)

The DST-OIB Tool will generate sustainment requirements based on the Sustainable Readiness Process and fleet maintenance strategies while integrating them with other maintenance workload such as modernization, foreign military sales, and joint requirements into a single demand signal. The DST-OIB Tool develops an integrated capacities/capabilities planner to simulate how AMC can leverage maintenance assets to meet demand. The automated capability enables risk assessment that describes how meeting the requirements improves operational readiness as well.

Depot Production Support Tool (DPST)

The Depot Production Support Tool provides visibility of Commander's Critical Information Requirements (CCIRs) related to Depot production.

Electronic Technical Manuals (ETMs) / Interactive Electronic Technical Manuals (IETMs)

Maintenance Readiness Metrics

The Maintenance and Readiness Metrics is a part of the SABRE Viz suite of visualizations and provide tactical, operational, and strategic views for a variety of dashboards supporting the Army's Monthly Readiness Reporting and daily Maintenance posture. Formerly found in the Army Readiness Common Operating Picture (AR-COP), these views include Fleet Readiness, Fleet Projection, Shop Operations, TMDE, EMSR, and Aviation Readiness dashboards.

Material Master / Enterprise Data Management Office View

Enterprise Data Management Office (EDMO) View of AEMM data

Materiel Enterprise Capability - Database (MEC-D)

The Materiel Enterprise Capabilities Database is a tool that captures, consolidates, and lists sustainment capabilities of the AMC Industrial Base down to the location level. This tool directly supports the revitalization of the OIB effort and its linkage to sustainable readiness. MEC-D aligns with requirements outlined in the Arsenal Act, 10 U.S.C. 4532Army and is a component of the strategic plan to address the CGs Strategic Focus Area Industrial Base Readiness. Additionally, the Materiel Enterprise Capabilities Database (MEC-D) is a tool used to simplify initial market research for manufacturing and repair capabilities within the Army Organic Industrial Base. Primary users of the MEC-D have US Army Acquisition and Sustainment requirements, but also include other DoD and USG requirements.

Materiel Visibility

The Materiel Visibility Metrics is a part of the SABRE Viz suite of visualizations and contains workbooks that are tied to visualizing the Army's materiel. Formerly found in the Army Readiness Common Operating Picture (AR-COP), these views include Army EOH Executive, IUID Metrics, Asset Visibility, LIN Visibility and Ammunition Executive workbooks.

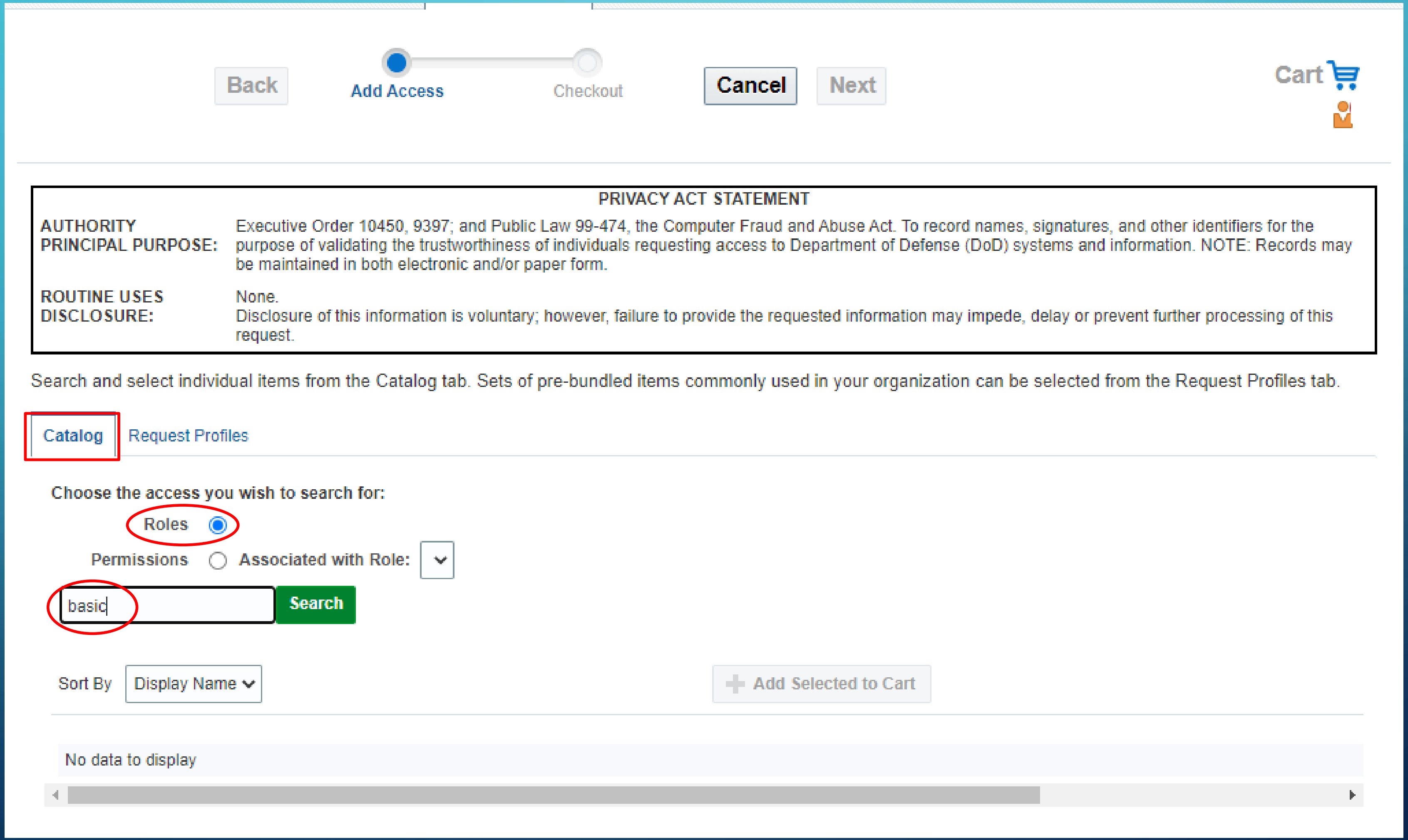
Modification Management Information System (MMIS)

MMIS enables users to determine the modification work order (MWO) status of their equipment down to the serial number level, as well as the ability to track safety of use messages (SOUMs) and ground precautionary advisories (GPAs). The use of MMIS for unit reporting is directed AR 750-10, Army Modification Program.

Organic Industrial Base (OIB) Metrics

The Organic Industrial Base (OIB) Metrics capability is part of the SABRE Viz suite and provides operational and strategic views of supply

MAKE SURE YOU ARE ON THE CATALOG TAB AND ROLES RADIO BUTTON. TYPE "BASIC" IN THE SEARCH BAR



PRIVACY ACT STATEMENT

AUTHORITY PRINCIPAL PURPOSE: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. 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.

Search and select individual items from the Catalog tab. Sets of pre-bundled items commonly used in your organization can be selected from the Request Profiles tab.

Choose the access you wish to search for:

Roles ●

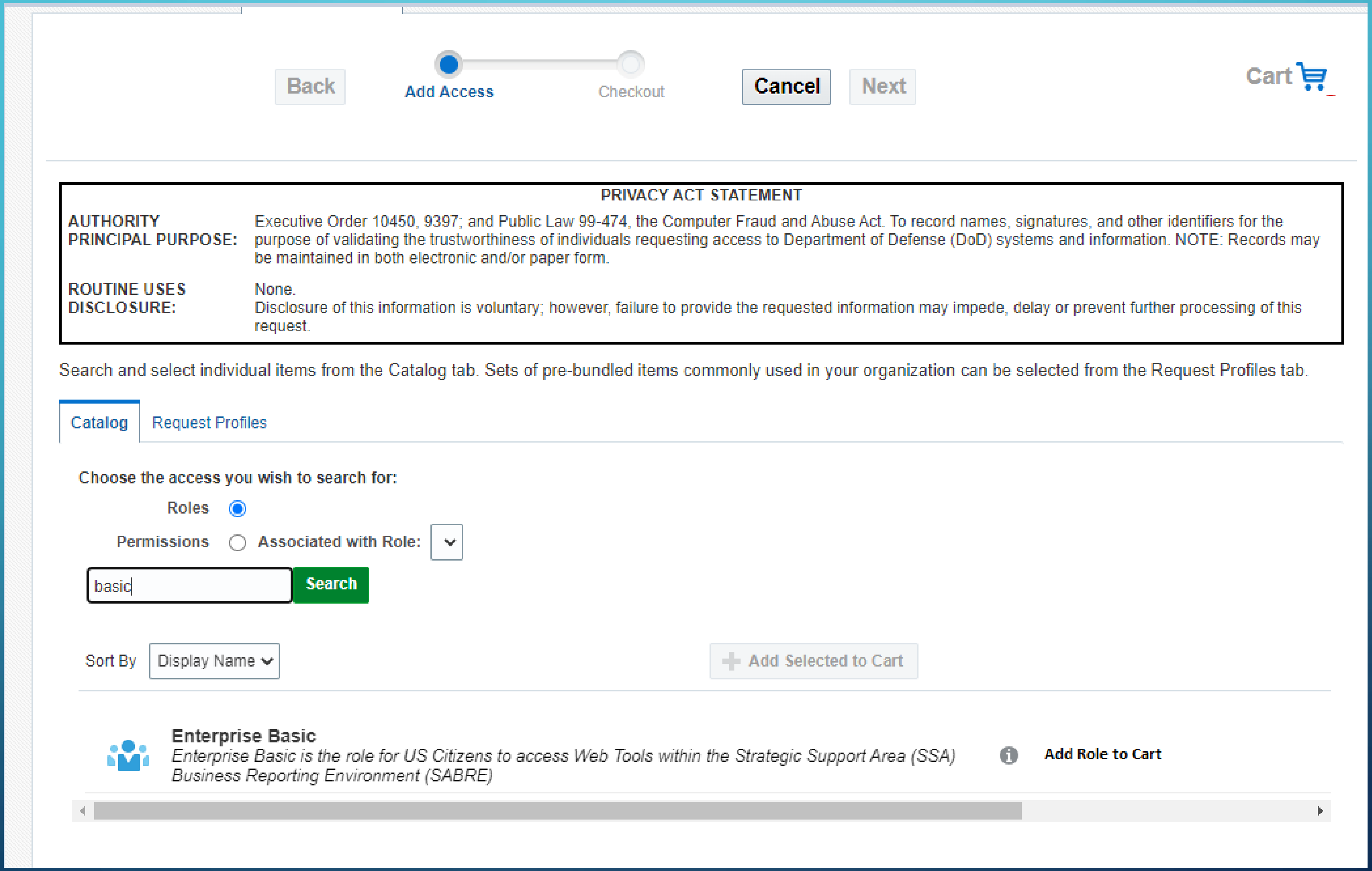
Permissions ○ Associated with Role:

basic

Sort By: Display Name

No data to display

CHOOSE ENTERPRISE BASIC AND CLICK "ADD SELECTED TO CART" AND THEN CLICK "NEXT"



PRIVACY ACT STATEMENT

AUTHORITY
PRINCIPAL PURPOSE:

Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. 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
DISCLOSURE:

None.
Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

Search and select individual items from the Catalog tab. Sets of pre-bundled items commonly used in your organization can be selected from the Request Profiles tab.

Choose the access you wish to search for:

Roles ●

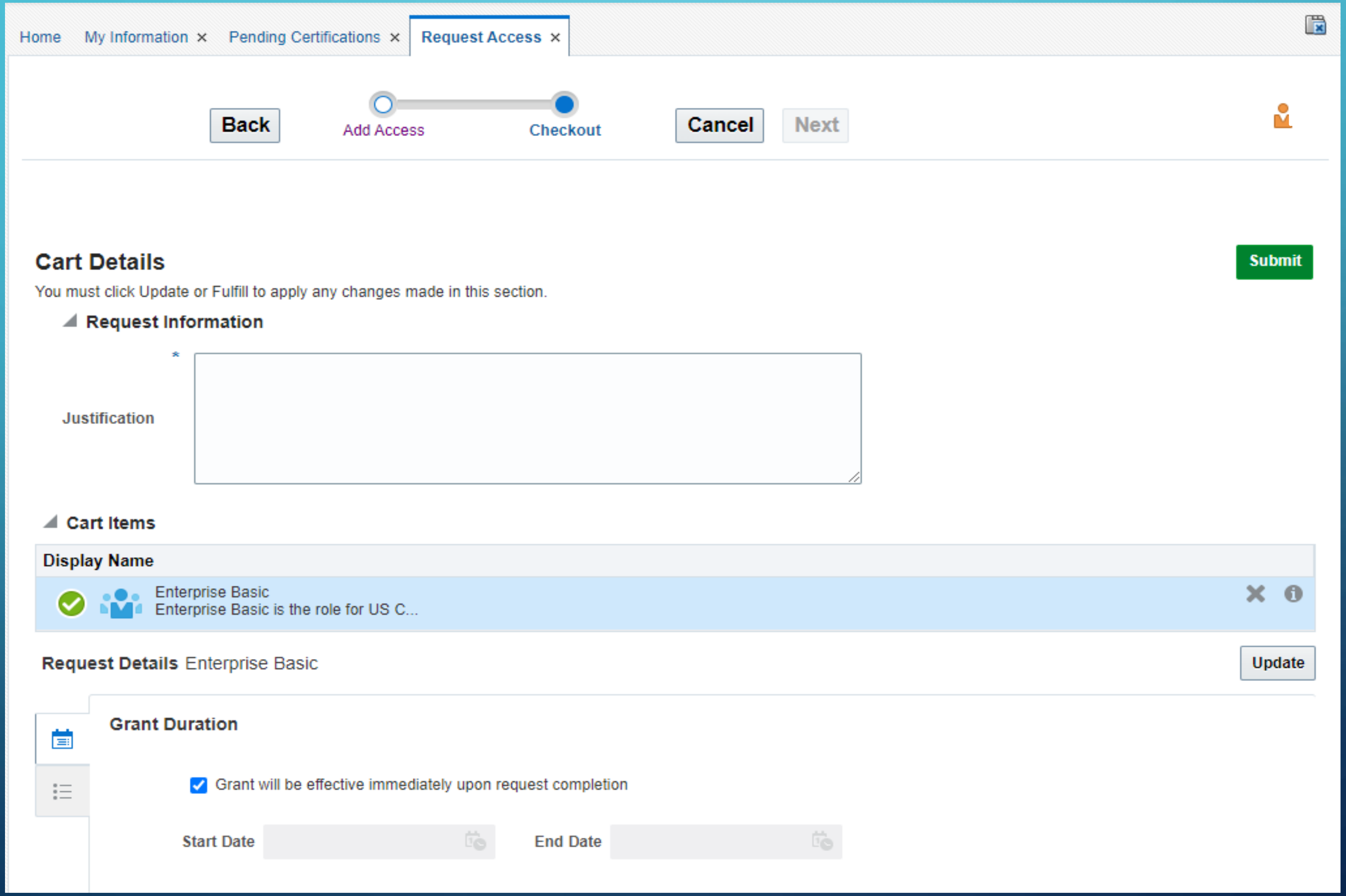
Permissions ○ Associated with Role:

basic

Sort By Display Name

Enterprise Basic
Enterprise Basic is the role for US Citizens to access Web Tools within the Strategic Support Area (SSA) Business Reporting Environment (SABRE)

FILL IN JUSTIFICATION. – “MLMC STUDENT” THEN CLICK “SUBMIT”



Cart Details

You must click Update or Fulfill to apply any changes made in this section.

Request Information

* Justification

Cart Items

Display Name
Enterprise Basic Enterprise Basic is the role for US C...

Request Details Enterprise Basic

Grant Duration

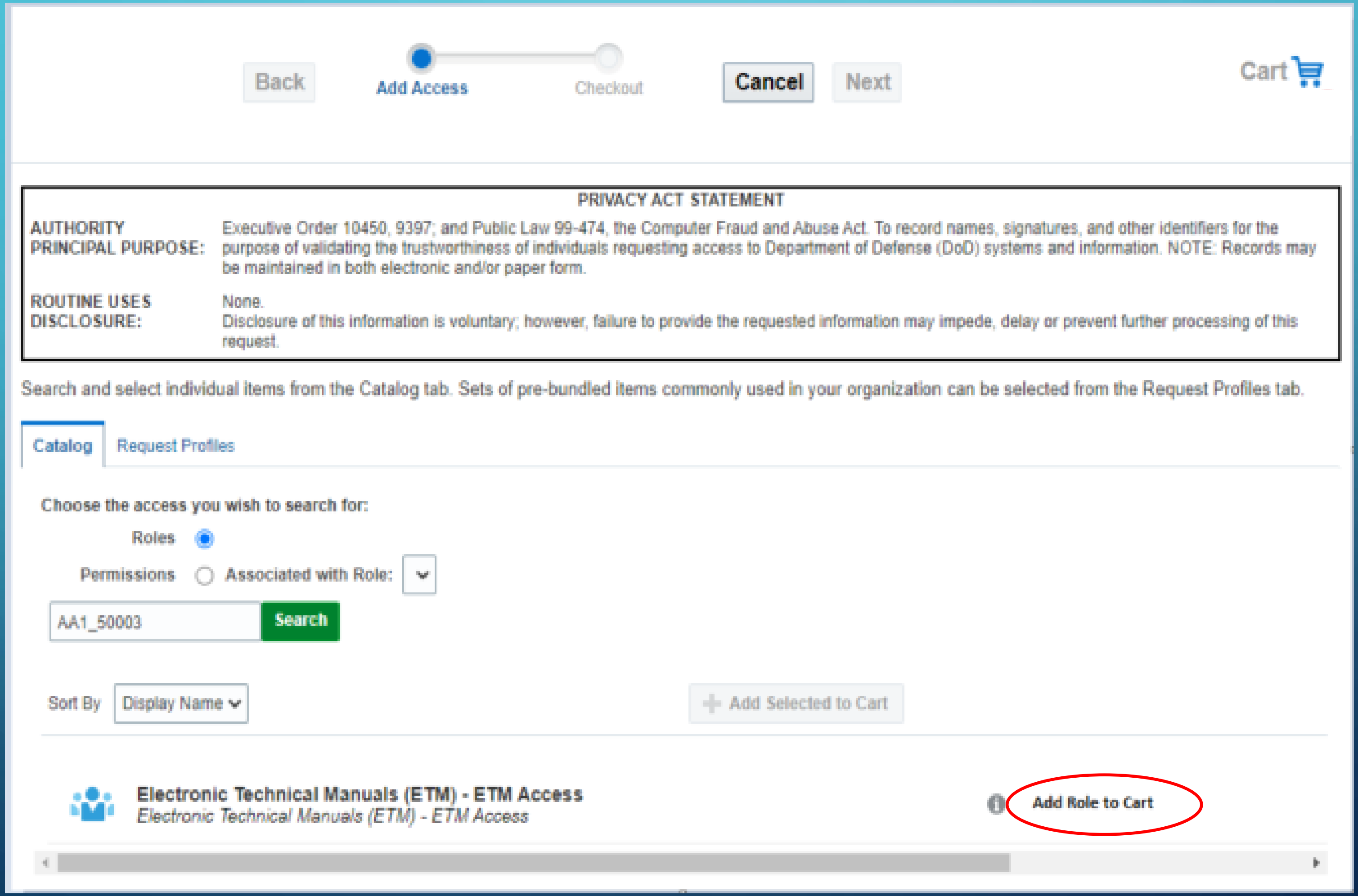
☑ Grant will be effective immediately upon request completion

Start Date

End Date

ETM'S - THE ENTERPRISE BASIC ROLE/LDAC SABRE TAB ALLOWS YOU TO SEE PUBLICATIONS/ETMS BUT DOES NOT GIVE YOU ACCESS TO IT.

ETMS -
PLEASE FOLLOW THE DIRECTIONS BELOW.
TYPE 50003 IN THE SEARCH BAR AND CLICK ON ADD ROLE TO CART



PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. To record names, signatures, and other identifiers for the

PRINCIPAL PURPOSE: 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.

Search and select individual items from the Catalog tab. Sets of pre-bundled items commonly used in your organization can be selected from the Request Profiles tab.

Choose the access you wish to search for:

Roles ●

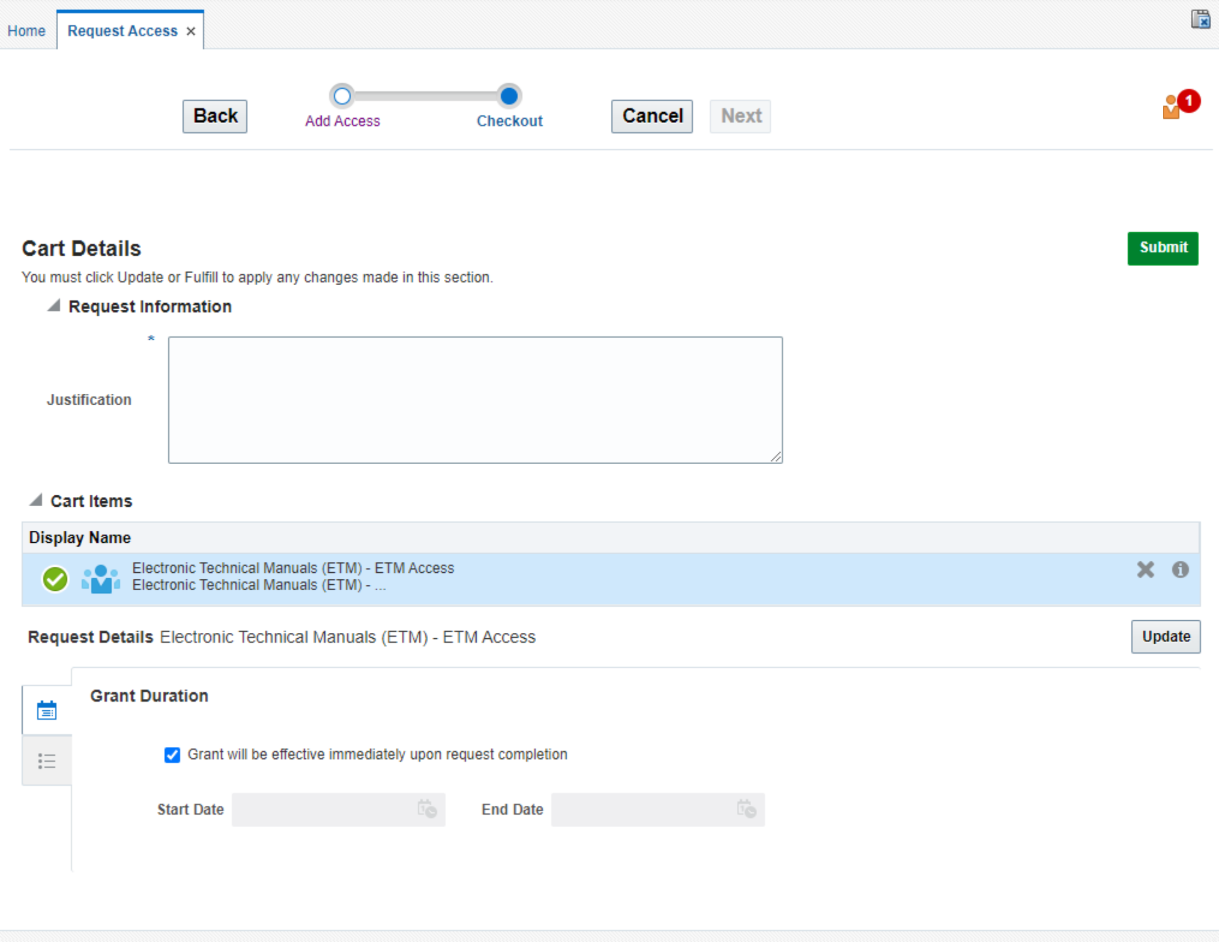
Permissions ○ Associated with Role:

AA1_50003 Search

Sort By Display Name

Electronic Technical Manuals (ETM) - ETM Access
Electronic Technical Manuals (ETM) - ETM Access

FILL IN JUSTIFICATION. - STATING THAT THE ROLE IS NEEDED “MLMC STUDENT”



Cart Details

You must click Update or Fulfill to apply any changes made in this section.

Request Information

* Justification	

Cart Items

Display Name
Electronic Technical Manuals (ETM) - ETM Access Electronic Technical Manuals (ETM) - ...

Request Details Electronic Technical Manuals (ETM) - ETM Access

Grant Duration

☑ Grant will be effective immediately upon request completion

Start Date   End Date

SAAR APPROVALS

- There are 4 levels that must be approved.
- After each approval, you will receive an email to confirm that the person has signed off.
- After the 4th level of approval, the SAAR then must be provisioned, this is historically done on Fridays.

1. Supervisor - Supervisors have 5 days to action a request or it will be escalated to the Supervisor’s Supervisor, who will have 5 days to action or the request will expire.
2. Security Officer - The SM / FSO will have 7 days to action a request after the Supervisor has approved the request or it will expire.
3. Functional/Data Owner - Functional Owners will have 7 days to action a request after the SM / SFO has approved the request or it will expire.
4. Cybersecurity/Information Assurance team - Cybersecurity team will have 7 days to action a request after the Functional Owner has approved the request or it will expire.

REGISTERING FOR AN ACCOUNT (IF YOUR SUPERVISOR OR SECURITY OFFICER DOES NOT COME UP WHEN YOU SEARCH, PLEASE SEND THEM THE INSTRUCTIONS BELOW SO THEY CAN REGISTER)

- Go to https://login.aesip.army.mil - Portal / IDM Landing Page
- Click the link under the "Need Access?" section.*Do not select external approver*
- Use you 16-digit Authentication Certificate (PIV) (DOD # and 6-digit contractor/military/civilian number) when prompted.
- This will complete the registration with a "Successful" message and an email will be sent out.

LDAC SERVICE DESK CONTACT INFO

Redstone Arsenal, Alabama

256-955-7716

DSN – 312-645-7716

usarmy.redstone.ldac.mbx.service-desk@army.mil