



Temporary Student Account Creation





Introduction

Effective May 1st, 2025, the Army Training and Certification Tracking System (ATCTS) is no longer supported. This TTP will cover the steps SOCOM, MEDCOM, and Air Force students will need to take to receive an account. This is a TEMPORARY process until the new account creation process system is finished.



Contents

Overview.....Page 4
Required Documents.....Page 5
Locating courses.....Page 6
Submitting 2875.....Page 14
Last step.....Page 20



Overview of the process

- If student can not access the IGA website below, the student must request dual tenant entitlements
 - Unit's entitlement manager
- Send required documents to NCOA S-6
 - Dalton.B.Lewis2.civ@army.mil
- Submit 2875
 - <https://iga.army.mil/identityiq/workitem/commonWorkItem.jsf>
- Submit New System Access Request
 - <https://www.aesmp.army.mil/>
- Approval and account creation
 - Supervisors and ISSO/ISSM's



Required Training and Documents

- Army Cyber Awareness Training Certificate
 - <https://cs.signal.army.mil/>
- Army IT User Agreement
 - <https://cs.signal.army.mil/>
- Records Management Training Certificate
 - <https://www.lms.army.mil>
- Controlled Unclassified Information Training Certificate
 - <https://www.cdse.edu/training>

In **ONE** email, please send your name, DOD ID, identify that you are permanent party or a student with graduation date, all required training completion certificates and Army IT user agreement to :
Dalton.B.Lewis2.civ@army.mil



DoD Cyber Awareness Training

1. Log-in to cs.signal.army.mil
2. On the FY25 DOD Cyber Awareness Training panel, select “Take Training”

FY 2025 DOD Cyber Awareness Training

This revised version of Cyber Awareness Challenge provides enhanced guidance for online conduct and proper use of information technology by DoD personnel. This training simulates the decisions that DoD information system users make every day as they perform their work. Rather than using a narrative format, the Challenge presents cybersecurity and information systems security (ISS) awareness instructional topics through first-person simulations and mini-game challenges that allow the user to practice and review cybersecurity concepts in an interactive manner.

You must click “Verify Training” at the end of the exam to gain credit. If your session has expired or was left idle for too long there is no way to retrieve the progress. The training will have to be taken again.

DoD released the FY25 Cyber Awareness training on 2 Oct 24. The FY 25 training is now accessible for completion.

Take Training

Mandated Army IT User Agreement

New IT User Agreement is posted to the site as of 23-MAY-2024

The purpose of this policy is to outline the acceptable use of computer equipment within a DoD/Army organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army units to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to the DoD/Army organizations.

Sign Mandated Army IT User Agreement

Download additional resources:

- [Facilitator Guide \(PDF\)](#)
- [Briefing Handout \(PDF\)](#)
- [Briefing Presenter Notes \(PDF\)](#)

At the end of your training, make sure to download a copy of the completion certificate.

Name the document:
YYYYMMDD_CUI_NCOA_DoDCyber
Awareness_lastname_firstname



Army IT User Agreement

- After completing the DoD Cyber Awareness Training, select “Sign Mandated Army IT User Agreement”

FY 2025 DOD Cyber Awareness Training

This revised version of Cyber Awareness Challenge provides enhanced guidance for online conduct and proper use of information technology by DoD personnel. This training simulates the decisions that DoD information system users make every day as they perform their work. Rather than using a narrative format, the Challenge presents cybersecurity and information systems security (ISS) awareness instructional topics through first-person simulations and mini-game challenges that allow the user to practice and review cybersecurity concepts in an interactive manner.

You must click "Verify Training" at the end of the exam to gain credit. If your session has expired or was left idle for too long there is no way to retrieve the progress. The training will have to be taken again.

DoD released the FY25 Cyber Awareness training on 2 Oct 24. The FY 25 training is now accessible for completion.

Take Training

Download additional resources:

- [Facilitator Guide \(PDF\)](#)
- [Briefing Handout \(PDF\)](#)
- [Briefing Presenter Notes \(PDF\)](#)

Mandated Army IT User Agreement

New IT User Agreement is posted to the site as of 23-MAY-2024

The purpose of this policy is to outline the acceptable use of computer equipment within a DoD/Army organization. These rules are in place to protect the employee and the organization. Inappropriate use exposes DoD/Army units to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to the DoD/Army organizations.

Sign Mandated Army IT User Agreement



Army IT User Agreement

- After reading the user agreement, fill out your information at the bottom of the webpage and select “Click to digitally sign”

(2) The user consents to interception, capture, and seizure of all communications and data for any authorized purpose (including PM, LE, or CI investigation). However, consent to interception, capture or seizure of communications and data is not consent to the use of privileged communications or data for PM, LE, or CI investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

(3) Whether any communications or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with

Personnel Type Required -- select an option --
Organization Required -- select an option --
Middle Initial *Leave blank if inapplicable.*

By my digital signature, I acknowledge that I have read, understand, and agree to the policies and procedures as defined in the mandated Army IT agreement
 I acknowledge and accept the mandated IT agreement.

Click to digitally sign

After digitally signing the Army IT User Agreement, make sure to download a copy.

Name the document:
YYYYMMDD_CUI_NCOA_Army ITUserAgreement_lastname_firstname

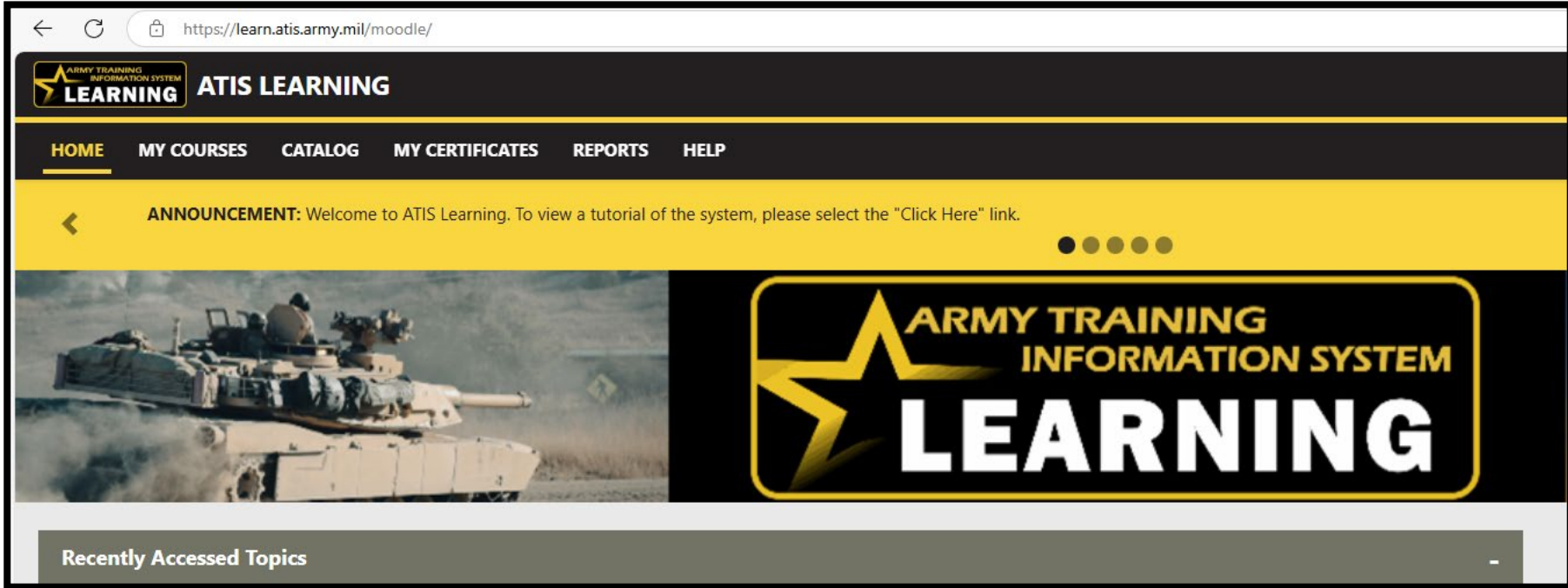


“LEADERS TRAINING LEADERS”



Records Management Training

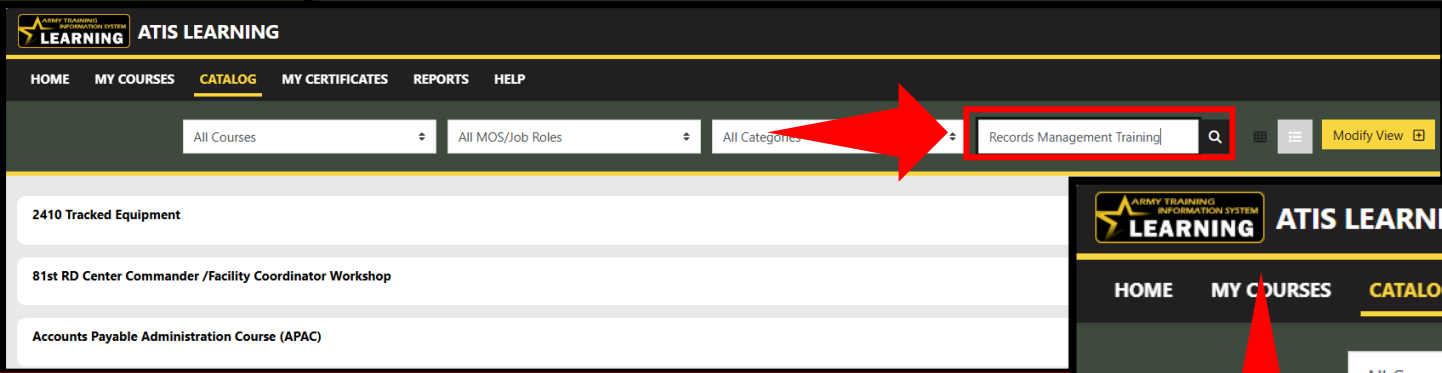
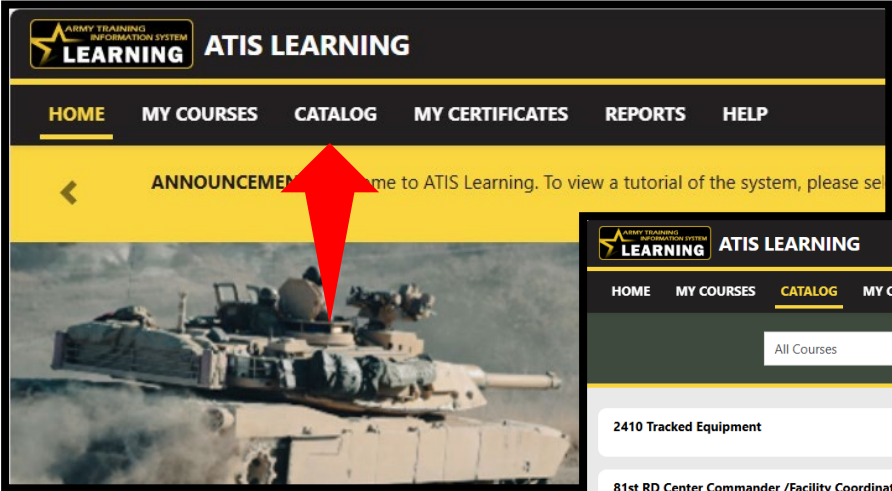
Log-in to <https://www.lms.army.mil>





Records Management Training

Select Catalog and then search “Records Management Training”. The exact course name is Records Management Training Course.



At the end of your training, make sure to download a copy of the completion certificate. Name the document:
YYYYMMDD_CUI_NCOA_RecordsManagementTraining_lastname_firstname



“LEADERS TRAINING LEADERS”



Controlled Unclassified Info Training

Log-in to <https://www.cdse.edu/training>

The screenshot shows the 'Training' page of the Center for Development of Security Excellence (CDSE). The header includes the organization's name, a search bar, and a 'STEPP Login' button. Below the header, there are navigation links: 'I'm interested in...', 'I'm looking for...', and 'I'm in need of...'. The main content area features a 'Training' heading, a link to 'Am I eligible to take CDSE training?', and two sections: 'Access training available on the Security Awareness Hub' and 'Access training available on STEPP'. At the bottom, there are four icons representing different course types: Curricula, eLearning Courses, Instructor-led Courses, and Virtual Instructor-led Courses, each with a brief description.



Controlled Unclassified Info Training

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

I'm interested in... I'm looking for... I'm in need of...

HOME > TRAINING

Training

Am I eligible to take CDSE training?

CDSE provides diverse security courses and Training is presented through a variety of learning methods for students. Don't see what you're looking for?

Access training available

- Annual Mandatory Training
- Controlled Unclassified Information (CUI) Training**
- Derivative Classification Training
- Marking Classified Information Training
- Operations Security (OPSEC) Training

Hover over “I’m in need of...” and then select “Controlled Unclassified Information (CUI) Training”. On the new webpage select the hyperlink “DOD Mandatory Controlled Unclassified Information (CUI)”

Controlled Unclassified Information (CUI) Training

eLearning

Internet-based, self-paced training courses

- DOD Mandatory Controlled Unclassified Information (CUI) Training**

This course is mandatory training for all of DOD personnel with access to controlled unclassified information (CUI). The course provides information on the eleven training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI along with the procedures for identifying and reporting security incidents. This course also fulfills CUI training requirements for industry when it is required by Government Contracting Activities for contracts with CUI requirements.



Controlled Unclassified Info Training

SECURITY AWARENESS HUB
Select eLearning awareness courses for DOD and Industry

DoD Mandatory Controlled Unclassified Information (CUI) Training

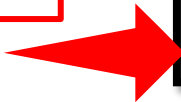
This course is mandatory training for all DoD personnel with access to controlled unclassified information. The course provides information on the eleven training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI along with the procedures for identifying and reporting security incidents. This course also fulfills CUI training requirements for industry when it is required by Government Contracting Activities for contracts with CUI requirements.

NOTES:

1. This course and exam may be taken an unlimited number of times.
2. Students will receive a certificate for the course after passing the exam with a 70% or better score. Please note, the exam must be completed in a single session because bookmarking is not available.
3. Students are encouraged to print or save a copy of the certificate as evidence of completion as CDSE does not maintain records of course completions from this site.
4. The course will run best in Edge Chromium, Google Chrome and MozillaFirefox. Pop-ups must be enabled.
5. For those using assistive technology, the following keyboard shortcuts have been added to this course:
 1. Press Ctrl + M to mute audio
 2. Press Alt + Right Arrow for the next screen and Alt + Left Arrow to go to the last screen
 3. Press tab to navigate interface elements of the course, and use the up and down arrow to explore instructional elements on each screen.

[Launch Course](#)

On the webpage that opens, select launch course



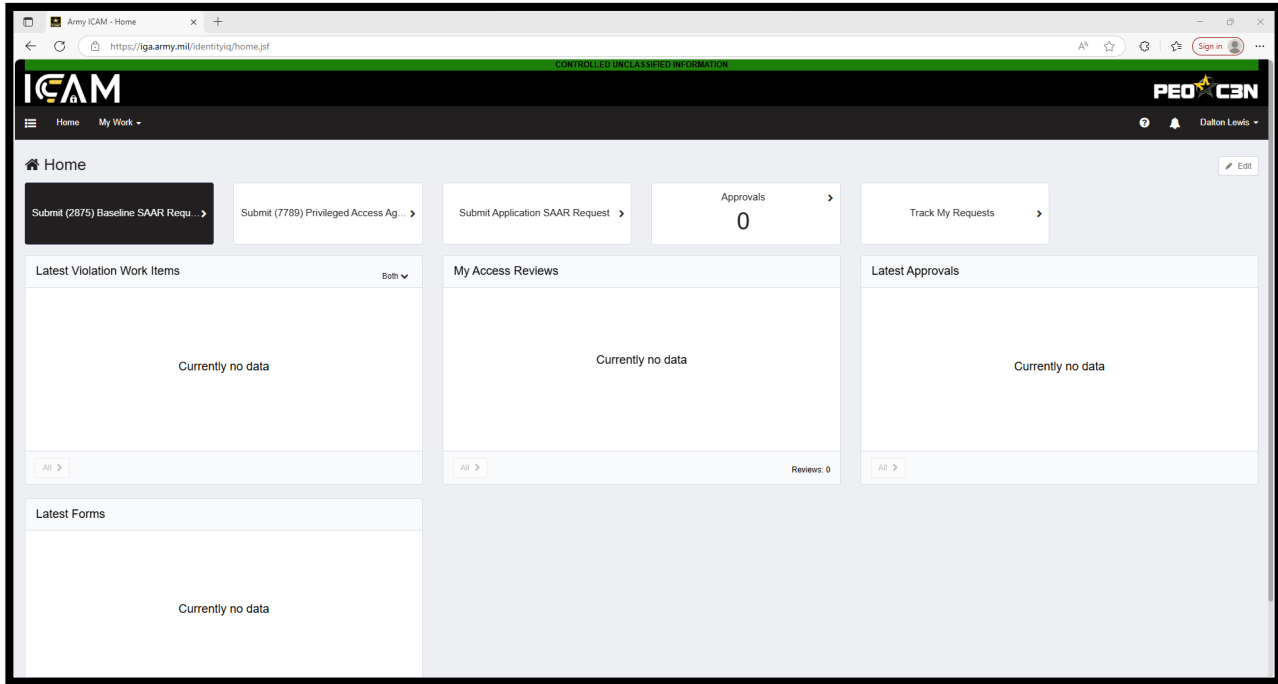
At the end of your training, make sure to download a copy of the completion certificate.

Name the document:
YYYYMMDD_CUI_NCOA_C
UIInfoTraining_lastname_firstname



Submitting Baseline 2875

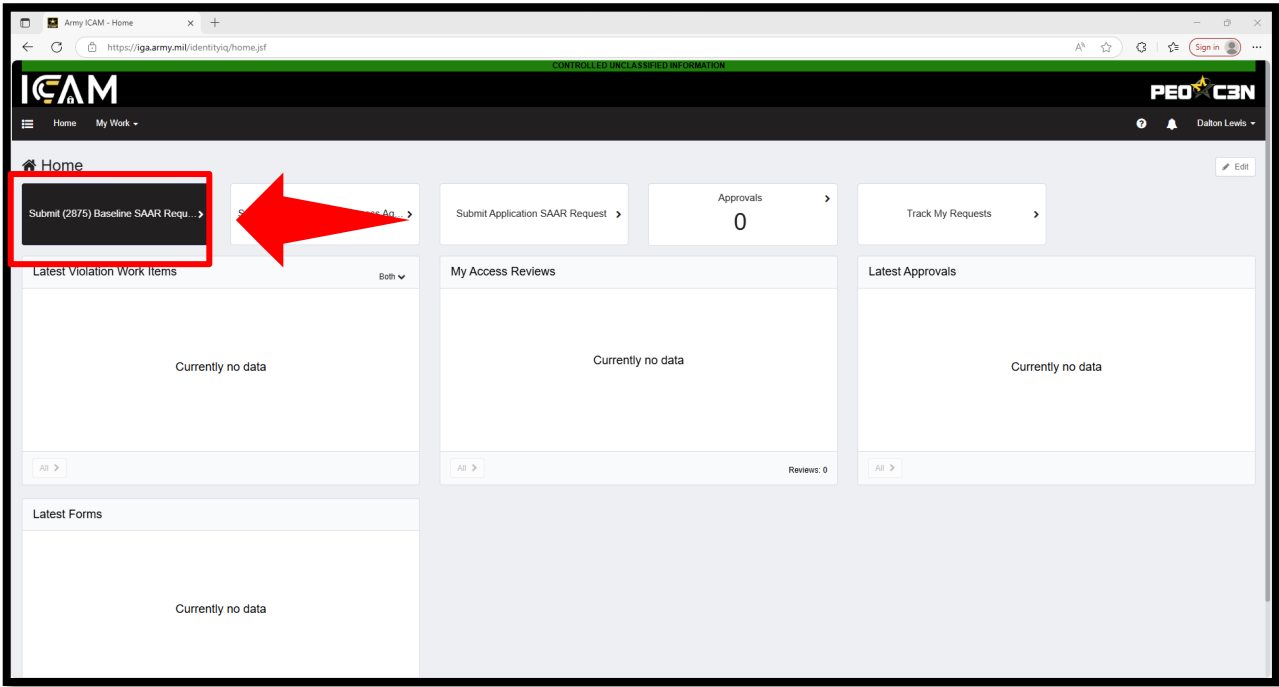
Sign-in to <https://iga.army.mil/identityiq/home.jsf>





Submitting Baseline 2875

Select “Submit (2875) Baseline SAAR Request”





Submitting Baseline 2875

Baseline System Authorization Access (2875) Form for: dalton.b.lewis2.civ

PRIVACY ACT STATEMENT
AUTHORITY: 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.

●○○○

Cancel Next >



Select which option works for your case

Baseline System Authorization Access (2875) Form for: dalton.b.lewis2.civ

Are you submitting for yourself or for another user? *

Myself
 Other

○○○○

Previous Cancel Next >



Review your information and select next

Baseline System Authorization Access (2875) Form for: dalton.b.lewis2.civ

User Account Information

Identity Name * dalton.b.lewis2.civ	DoD ID / EDIPI : [REDACTED] <small>(Electronic Data Interchange Personal Identifier)</small>	First Name Dalton <small>First Name of user requesting</small>
Last Name Lewis <small>Last Name of user requesting</small>	Branch of Service A <small>(Army, Air Force, Navy)</small>	Designation of Person CIV <small>i.e (Military, Civilian, Contractor, etc..)</small>
UIC W43LAA	Organization : USARMY <small>User Current Organization</small>	Office Symbol/Department USARMY 7ATC-NCOA <small>Office Symbol/Department of user requesting</small>
Official Email Address [REDACTED] <small>Official Email Address of user requesting</small>	Official Mailing Address Bavaria <small>Official Mailing Address of user requesting</small>	Phone [REDACTED] <small>Phone of user requesting</small>
Job Title IT Specialist	Citizenship USA	

○○○○

Previous Cancel Next >





Submitting Baseline 2875

Baseline System Authorization Access (2875) Form for: dalton.b.lewis2.civ

Account Request Information

Request Created : 05/06/2025

Network Access Requested :

Justification For Access : *

Supervisor/Sponsor Email : *

Security Manager Email :

ISSO or Appointee Name :

Annual Cyber Awareness Training Date : 06/20/2024

Derivative Classification Completion Date :

Agreement date provided must be within the past 11 months from the request date.

Please note that all fields with a red asterisk are required.

You must fill all required fields before submitting.

Previous Cancel **Select Submit** Submit

Select NIPR

Require NIPRNET to perform duties while assigned as a student at the 7th ATC NCOA

Your supervisor's email or assigned Academy Small Group Leader's Email

Dalton.B.Lewis2.civ@army.mil

Check date of training on cs.signal.army.mil

Your unit's Security Manager (Contact your G2/S2)

Check date of training on cs.signal.army.mil

After selecting submit, contact your supervisor to approve your 2875



Submitting AESMP Ticket

- Navigate to <https://www.aesmp.army.mil>
 - Search “new system access request”
 - Select this option



The screenshot shows a search result for "new system access request". The top result is "Dashboard - New System Access Request". Below it, a knowledge article is highlighted with a red border:

Knowledge & Catalog - Knowledge (8 of 489)		
AESMP Customer Support: How to Request Access to a System, NIPR, or SIPR Account (New System Access Request (NSAR) / DD2875 Process)		
Category	Number	Updated
Customer Support	KB0014366	2025-04-24 23:59:57

The instructions below guide you through the process of filling out the New System Access Request (NSAR) form to request NEW access to a system, or a new NIPR, or SIPR account. IMPORTANT: The following requirements need to be completed BEFORE submission of the NSAR form. Valid 2875 (SAAR) or 7789 (Privileged Access Agreement) in AVS NOTE: As of...



Submitting AESMP Ticket

This page has a video and step-by-step instructions on how to submit your access request.

AESMP Customer Support: How to Request Access to a System, NIPR, or SIPR Account (New System Access Request)
KB0014366 - [Latest Version](#)
39531 views

Introduction

The instructions below guide you through the process of filling out the New System Access Request (NSAR) form to request NEW access to a system, or a new NIPR account.

IMPORTANT:

The following requirements need to be completed BEFORE submission of the NSAR form.

1. Valid 2875 (SAAR) or 7789 (Privileged Access Agreement) in AVS
NOTE: As of 1 May 2025, ATCTS is now read-only access as the Army migrates to the Account Validation System (AVS). Therefore, if you do NOT have a current SAAR, you must complete the instructions on this new process
2. Your User's Agreement is current and not expiring within 30 days
3. Your Cyber Challenge training shows as current within 12 months, and not expiring within 30 days, in AVS
4. **For any SIPR access requests, the Derivative Classification training is to be attached to the request and is current within 12 months**
NOTE: Users with **INTERIM Secret** or **Top-Secret Clearance** (CIV or CTR) CANNOT receive a SIPR account until your Clearance has been confirmed
5. Other documents attached to the request, as required by policy (e.g., elevated privileges) for the requested access

Additional Information

- Click [HERE](#) to view the NETCOM 2024-06 Policy Change for DD2875
- Click [HERE](#) to view the NETCOM 2875 Directive FAQ and Updates SharePoint Site

Step one of the guide is the link to request access to a new systems, where you will fill out the form needed to submit your ticket.



Last Step

Once you have emailed your certificates, submitted your 2875 and, submitted your AESMP Ticket; send a confirmation email to your supervisor and Dalton.B.Lewis2.civ@army.mil



Click to edit Master title style

- Click to edit Master text styles
 - Second level
 - Third level
 - Fourth level
 - Fifth level