



HOW TO SUBMIT SAAR THROUGH AVS

Memo from the Director, Southeast Region Network Enterprise Center-Fort Stewart



CUI



DEPARTMENT OF THE ARMY
SOUTHEAST REGION NETWORK ENTERPRISE CENTER
87 MAYNARD ROAD (BUILDING 03)
FORT STEWART, GEORGIA 31314



All users are required to complete a System Authorization Access Request (SAAR) in the Account Validation System (AVS) by 20 September 2025. For new users only once, the SAAR has been completed, users must create an Army Enterprise Service Management Platform (AESMP) case to request new system access. **new users must request entitlement from DEPO manager before AVS can be completed.

1. Visit [ATCTS Sunsetting](#) for the latest guidance and changes.
2. CCoE G6 added a new tab [User Compliance Check](#) on the Cyber Awareness site. User's Cyber Awareness training and Information Technology User Agreement (IT UA) completion date can be searched using EDIPI.
3. AESMP New System Access Request Training [ATIS Training](#).
4. Training Certificates
 - i. Annual Cyber Awareness Training- [CS Signal Training Site](#)
 - ii. Annual Mandated Army IT User Agreement - [CS Signal Training Site](#)
 - iii. SIPR Only- Annual Derivative Classification Training- [Derivative Classification](#)
 - iv. Priv ledged Only: Annual Privileged User Cybersecurity Responsibilities [Privileged User Responsibilities](#)
5. AVS Account Management portal ([ICAM- AVS Portal](#)) All users will submit Baseline System Authorization Access (2875) Form.
6. Users will submit a ticket for account access. AESMP Request Portal or ServiceNow ([AESMP- New System Access Request](#)).
7. Privilege Level Access Requirement
 - a. Mission Partners- Must be a member of [Trusted Agents Teams Channel](#)
 - b. SAAR and PAA – completed in AVS
 - c. Upload required documentation to [IMO PLA Documents Repository](#)
 - i. SAAR and PAA (completed in AVS; a PDF of the approval is acceptable)
 - ii. Cyber Security Fundamentals certificate (Completed every 3 years)
 - iii. Annual Privileged User Cybersecurity Responsibilities certificate
 - iv. SCIP certificate of completion
 - v. DoD Cyber Workforce (DCWF) requirements per DoD 8140. DCWF work role training foundations and residential certificate of completion, and signed DCWF Appointment Orders

GIZA,STEPHEN.P
AUL.1061433151
Digitally signed by
GIZA,STEPHEN.PAUL.10614331
51
Date: 2025.06.24 14:53:20 -0400

STEPHEN P. GIZA III
Director, Southeast Region Network
Enterprise Center - Fort Stewart

CUI



- **By 20 September 2025, everyone needs to complete the new digital SAAR forms and Privilege Access forms (DD2875 SAAR & DA7789 PAA) via AVS. If this is not completed by this date the users account will be disable.**
- **ID Card Office Online Work Profile(CIV/MIL) profile must be updated with current Duty Organization information prior to submitting AVS request. (CAN TAKE UP TO 48 HOURS FOR UPDATED INFORMATION TO POPULATE IN AVS).**
- **<https://idco.dmdc.osd.mil/idco>**



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

Home My Work

Jason Lynch

Home

Edit

Submit (2875) Baseline SAAR Request for Self

Submit (7789) Privileged Access Agreement (PAA) ...

Submit Application SAAR Request

Approvals
0

Track My Requests

Latest Violation Work Items

Both

Currently no data

All

My Access Reviews

Reviews: 0

Latest Approvals

All

Latest Forms

Currently no data

All

Click on Submit
(2875) Baseline
SAAR Request for
Self.



Baseline System Authorization Access (2875) Form for [REDACTED]

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 Click on Next  Next >

Baseline System Authorization Access (2875) Form for: [REDACTED]

Are you submitting for yourself or for another user? *

☒ Myself Click on either Myself for a self submission or other if you're submitting on behalf of someone.

☐ Other

○○●○○

< Previous Cancel Click on Next  Next >

Baseline System Authorization Access (2875) Form for: [REDACTED]ctr

Are you submitting for yourself or for another user? *

☐ Myself

☒ Other

Email of User : *

[REDACTED]

Enter the email of the user you would like to request on behalf of.

Identity Found? *

[REDACTED]ctr

This field will auto-populate if the email address above is a valid DOD email.

○○●○○

< Previous Cancel If you're submitting on behalf of someone, type in their email address information without @army.mil and click on the  Next >

If you're submitting on behalf of someone, type in their email address information without @army.mil and click on the next button.



Baseline System Authorization Access (2875) Form for: [REDACTED]

Would you like to Update information from a previous Baseline 2875 Request? *

☐ Yes

☒ No

Always select no if you submitting for someone or your self.

Progress indicator: 4 circles, 3rd is filled.

Navigation: Previous, Cancel, Next >

Your User Account Information is pulled from ID Card Office Online. If this information is incorrect go to <https://idco.dmdc.osd.mil/idco> and update your MIL profile.



Baseline System Authorization Access (2875) Form [REDACTED].mil

User Account Information

Identity Name * [REDACTED].mil	DoD ID / EDIPI : [REDACTED] (Electronic Data Interchange Personal Identifier)	First Name [REDACTED] First Name of user requesting
Last Name Munoz Last Name of user requesting	Branch of Service A [REDACTED] (Army, Air Force, Navy)	Designation of Person MIL i.e.(Military, Civilian, Contractor, etc..)
UIC WNEUX1 UIC	Organization : USARMY User Current Organization	Office Symbol/Department USARMY 335 Sig Cmd Office Symbol/Department of user requesting
Official Email Address [REDACTED].mil@army.mil Official Email Address of user requesting	Official Mailing Address Reserve Official Mailing Address of user requesting	Phone Phone of user requesting
Job Title INFO TECH NCO	Citizenship USA	

Progress indicator: 4 circles, 3rd is filled.

Navigation: Previous, Cancel, Next >

Click on Next



Cyber awareness training and Army IT user agreement can be completed at :

<https://cs.signal.army.mil>



Baseline System Authorization Access (2875) Form for: [REDACTED]

Account Request Information

Request Created :

07/10/2025

Network Access Requested : *

Choose NIPR

Justification For Access : *

Fill out the justification

Fill out with supervisors
@army.mil email.

MWR ISSO
Wingate, Kerry T Jr.
kerry.t.wingate.naf@army.mil
Brown, Frederick D
frederick.d.brown38.naf@army.mil

Please provide date for your
IT User Agreement Date

If updating a previous request, please enter the approver (Supervisor and Security Manager) details before updated request details.

Supervisor/Sponsor Email : *

Security Manager Email :

Brigade Security Manager
Mr. Kenneth R. Miller
kenneth.r.miller80.civ@army
.mil

Enter the Supervisor's/Sponsor's email address, must be a Government Employee (CIV/MIL/NAF/NFG).

Enter the Security Manager's email address, must be a Government Employee (CIV/MIL/NAF/NFG/CTR).

ISSO or Appointee Name :

Annual Cyber Awareness Training Date :

Please provide date for your
Cyber Awareness Training

Enter the Information System Security Officer (ISSO) or Appointee's email address.

Please note this date is provided from <https://cs.signal.army.mil/>. Please allow 24-48 hours after submission to see updated information. Training date provided must be within the past 11 months from the request date.

Army IT User Agreement Date :

Derivative Classification Completion Date :

LEAVE THIS SPACE BLANK

Please note this date is provided from <https://cs.signal.army.mil/>. Please allow 24-48 hours after submission to see updated information. Agreement date provided must be within the past 11 months from the request date.

Please enter the user's completion date for the Derivative Classification training.

* denotes a required field

You must fill all required fields before submitting.

○○○○●

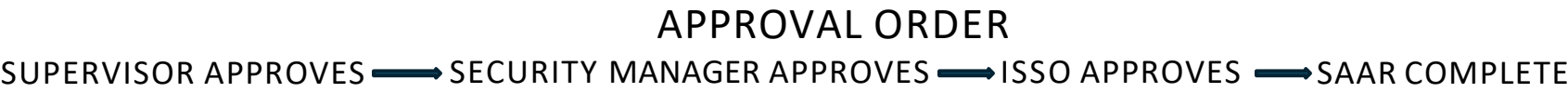
< Previous

Cancel

Submit



Once your SAAR is submitted an email will be sent for approval in the order below.



Home

Submit (2875) Baseline SAAR Request for Self >

Submit (7789) Privileged Access Agreement (PAA) ... >

Submit Application SAAR Request >

Approvals
0 >

Track My Requests >

Latest Violation Work Items Both ▾

My Access Reviews

Latest Approvals

Currently no data

Currently no data

Currently no data

All >

All > Reviews: 0

All >

You can track your request's by clicking on "Track My Requests"



Request Access: [redacted]

Requested by Jason Lynch on 5/1/25 | Request [redacted]

Details >

Request pending

Add Network Type: SIPR (inclusive of NIPR) on 2875 Network Request

Waiting

Cancel Request



Here is your request details where you can see where in the chain the account request is.



Your AVS SAAR is now complete.

AVS SAAR Request must be renewed for the following reasons:

- Upon PCS to a new duty station.
- Upon renewal of annual requirement to sign the Acceptable Use Policy (AUP).
- Upon renewal of annual requirement to complete Cyber Security Awareness training.
- Change of persona type (e.g. .mil to .civ; .civ to .ctr; .ctr to .mil; etc.).
- Change of last name.
- Upon renewal or extension of contracts.

The screenshot shows the ICAM web application interface. At the top, there's a navigation bar with 'Home' and 'My Work' links. The main header displays 'Access Requests' with a notification icon. Below this, a search bar and sorting options are visible. The central content area shows a request for 'Pablo Munoz' with the status 'Request completed on 6/11/25'. A green bar highlights the completion status, and a 'Complete' button is present. The bottom of the interface shows a pagination bar indicating 'Showing 1-1 of 1'.

Note: If you require any additional assistance or have any questions, please contact Automation personnel.

When you or your supervisor gets an email stating that the authorization was approved, follow the next steps to have your account created.



Proceed to part 2 only after you receive a notification that your authorization was approved



PART 2. Requesting account creation

This part must be completed by the new account requestor. Use a secondary cac reader to log into AESMP, or use a Kiosk image computer in the library.

1. Click [HERE to access the New System Account Request form in AESMP](#)

2. Fill-in the mandatory Requestor fields with your most applicable information.

3. Please type *W0VAAA.
and pick United States Army Garrison,
Fort Stewart

4. Check this box.

* Indicates required

* Requester Name

* Please provide your Service Component Type

* Duty Station/Duty Station UIC

Start typing "*" (asterisk) PLUS your location, organization, or the closest IT support organization to you. For example, *Rock Island *Schofield *82D *Nashville *W059AA

Note: Not all UICs have dedicated support organizations.

* Physical Location

* Building

* Room/Cubicle

* Normal Business Hours

* This determines who will receive your ticket to work it in the system.

☐ Did you update the field above to show where you are PHYSICALLY located now?

Requester Email Address

Requester Phone Number

* Requester Best Contact Number



5. Scroll down to the Is your 2875 (SAAR) or 7789 (Privileged Access Agreement) completed in AVS? and **select Yes.**

Important: You will NOT be able to proceed with your request until you have fully completed and signed DD2875 form in AVS .

* Is your 2875 (SAAR) or 7789 (Privileged Access Agreement) completed in AVS? 

Access AVS here. 

Yes 

6. In the What Army system are you requesting access to? drop-down field select NIPR Account.

7. **Click Next.**

* What Army system are you requesting access to?

4

NIPR Account 

5

Next



8. In the Please describe your access need field: Type I am requesting a new **NIPR Account**.

* Please describe your access need ?

Include any required attachments for your system owner at the bottom of this form. ✕

9. Type the @army.mil email address of your supervisor in the Provide the email for your supervisor field.
Important: It must be an @army.mil address of a user in the Army Global Address List (GAL) and MUST contain either .MIL, .CIV, or .NAF.

Example: Firstname.Lastname.CIV@army.mil

* Provide the email for your supervisor ?

This must be a valid .mil email address of a user in the Army Global Address List (GAL). ✕



10. Type the @army.mil email address of your ISSM or ISSO in the Provide the email address for your ISSM (Information System Security Manager) or ISSO (Information System Security Officer) field.

Note: MWR ISSO: kerry.t.wingate.naf@army.mil, frederick.d.brown38.naf@army.mil

* Provide the email address for your ISSM (Information System Security Manager) or ISSO (Information System Security Officer) ?

This must be a valid .mil email address of a user in the Army Global Address List (GAL).



11. Optionally, populate the Comments field with any additional information you think may be needed to fulfill your request.

Important: Please do not disclose any unnecessary Personally identifiable Information (PII) or any information that can be Classified.

Disclaimer ?

Please do not disclose any **unnecessary Personally Identifiable Information (PII)** or any information that can be **Classified**.



If you have a SIPR related request, please contact AESD-W-SIPR at 866-335-2769.

* Comments:

Please create an AUDS account and Active Directory account to be able to scan.



Fill out with the same wording



12. Click Submit to complete the request.

Submit

13. Upon successful submission you receive a Case number via a green banner at the top of the screen, and you will be notified via email when your request has been fulfilled.

Request associated to: CS3526891