



DEFENSE SECURITY
COOPERATION AGENCY

Security Through Global Partnerships

SCMS ICAM Registration

Presented by:
SCIP Development Team

Office of Business Operations/IM&T
September 1st 2026

UNCLASSIFIED





SCMS SAAR

- Go to DoD E-ICAM to start the process: <https://spnfm01-acc.icam.disa.mil/identityiq/home.jsf>
- Click the 3 lines to expand the left-side menu, click the “Manage Access” dropdown, and then click “Manage User Access”.
- Alternatively, you can click “Manage My Access” on the home page to get started on your request.

DoD E-ICAM 26-08 PRD

Notice: Upcoming changes with R26-08 will impact in-flight Access Requests. If not fully approved by 160, need to be resubmitted



Home My Work Intelligence

Home

Manage User Access >

Track My Requests >

Latest Violation Work Items Both v

Currently no data

All >

My Access Reviews

Currently no data

All >

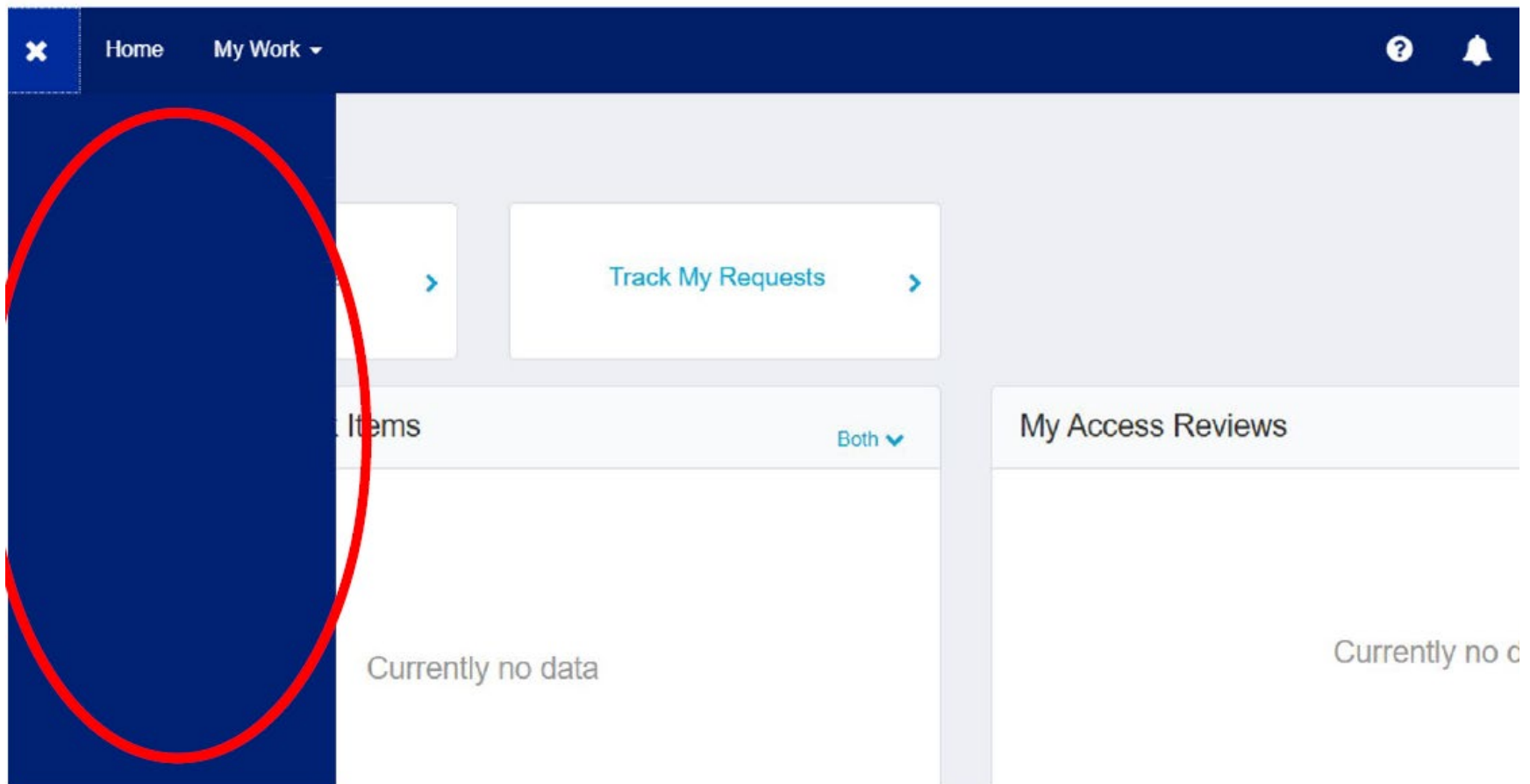
Reviews: 0



SCMS SAAR

Troubleshooting Steps

- If the menu is blank, close all open internet browsers and re-open DoD E-ICAM.
- If this doesn't work, clear your browser cache, close your browser window, and re-open it.
- When options appear in this menu, continue to the next slide.





SCMS SAAR

- To narrow the list of roles, click the **Filters** button and type “SCMS” in the Role Source Application filter.
- Wait several seconds for the results to display and select “SCMS AS” and click Apply.



Home My Work ▾ Intelligence ▾

Manage User Access

1 Select Users

Find and select users for whom you want to manage access.

2 Manage Access

Add access for the users you've selected.

3 Review and Submit

Look over your selections and confirm.

Add Access

Remove Access

Search By Keywords ▾

Search Access



Filters ▾

Identities Selected: Garrison, Matthew CIV DSCA OBO IMT PEO-CLS (USA)

Showing 1-12 of 100

Filter Access

Role Source Application

SCMS AS

SCMSTEST AS

Clear

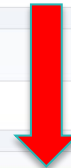
Apply



SCMS SAAR

- Click the checkmarks to select the user role(s) which you are requesting access. For role descriptions, select the **Details** button to the right of the role.
- For basic access to SCMS, select “General Base Support (Required)”. Wait several seconds, and the checkmark will eventually display as green when selected.
- When finished selecting your desired role(s), click the **Next** button.

☒	General Base Support (Required)	Details
Type:	Role	Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false
☐	LIMITED NSR Support	Details
Type:	Role	Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false
☐	Manager Support	Details
Type:	Role	Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false
☒	MOA Tranche Support	Details
Type:	Role	Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false
Previous Next		





SCMS SAAR

- To the right of your selected role(s) is a paperclip and speech icon.
- Select the paperclip icon to upload attachments. For roles requiring uploaded documentation, this icon will be marked with a red asterisk.
- Select the speech icon to enter comments.
- If the paperclip icon displays a red asterisk, select it and upload your Cyber Security certificate (PDF only).

Add Access 1

✕ General Base Support (Required)

Type: Role Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false

  Details



Previous

Cancel

Submit



- To attach documentation, you may either drag and drop or click the hyperlink to upload a file. DoD E-ICAM displays the uploaded file and provides the opportunity to enter a file description.
- NOTE:** Supervisors are responsible for verifying the attached files. DoD E-ICAM does not validate PDF content. All uploaded files are included in the Supervisors email notification for the request.

Attach a File to General Base Support (Required)



Drag and drop file here

[Or click to upload a file](#)

2 Manage Access
Add access for the users you've selected

3 Review and Submit

Attached to This Item

No Attachments



SCMS SAAR

- When all required attachments have been uploaded, click the **Submit** button to move your request to the next step.

Add Access 1

☐ General Base Support (Required) Details

Type: Role Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false

Previous Cancel Submit

A large red arrow points downwards from the top of the form area towards the "Submit" button at the bottom.



SCMS SAAR

- Click **Complete Form** to move to the next step.

DoD E-ICAM 26-08 PRD

DISA

Home My Work Intelligence

Manage User Access

1 Select Users
Find and select users for whom you want to manage access.

2 Manage Access
Add access for the users you've selected.

Review and Submit
Review your selections and confirm.

Identities Selected: Garrison, Matthew CIV DSCA OBO IMT PEO-CLS (USA)

Add Access 1

MOA Tranche Support

Type: Role Access Type: AUTHORIZED Appointment Letter: false Authorization Letter: false Privileged User Agreement: false

More Info Needed

More information is needed to complete your request. Fill out the form to provide additional information.

Identity: Garrison, Matthew CIV DSCA OBO IMT PEO-CLS (USA)

Later Complete Form

Help

Normal

Details



- Review the Privacy Act Statement and click **Next** to move to the next step.

Complete Work Item

System Authorization Access Request (SAAR) - User Request

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

Return Later

Cancel Request

Next >





SCMS SAAR

- Review and populate any required fields (indicated by a red asterisk). Most fields should be pre-populated.
- **Type of Request** – Initial or Modification. The system pre-selects **Initial**. Adjust to **Modification** if you have already submitted an E-ICAM SAAR for SCMS.
- **Supervisor Email** – If the Supervisor information is not auto-populated, enter your Supervisor's email address in this field. If the email address is found in the database, the system will auto-populate the **Supervisor Name** field.
- Click **Next** to move to the next step.

Complete Work Item

System Authorization Access Request (SAAR) - User Request

Data Source WARNING:

*** Incorrect user data may only be updated at the RAPIDS ID Card Office Online: <https://idco.dmdc.osd.mil/idco/>

TYPE OF REQUEST *

- ☐ INITIAL
☒ MODIFICATION

NAME *

Garrison, Matthew CIV DSCA OBO IMT PEO-I

PHONE

(223) 758-3355

If phone cannot be validated please select None.

OFFICIAL MAILING ADDRESS *

Naval Support Activity Mechanicsburg,
PA

ACCESS EXPIRATION DATE

mm/dd/yyyy

SUPERVISOR NAME *

Gandy, Chad R CIV DSCA OBO IMT PEI

SYSTEM LOCATION

(Location of system)

ORGANIZATION *

dsca

OFFICIAL EMAIL ADDRESS *

matthew.garrison5.civ@mail.mil

CITIZENSHIP *

US

SUPERVISOR EMAIL *

chad.r.gandy.civ@mail.mil

(Supervisor Email search)

TYPE OF ACCESS REQUIRED: *

AUTHORIZED

OFFICE SYMBOL/DEPARTMENT *

DSCA OBO IMT PEO-CLS

JOB TITLE AND GRADE/RANK *

IT Specialist (SYSANALYSIS)

DESIGNATION OF PERSON *

CIV

● ○ ○ ○ ○

< Previous

Return Later

Cancel Request

Next >



- Review the Access Selection and click **Next** to move to the next step.

Complete Work Item

Request on Behalf: System Authorization Access Request (SAAR) - User Request

Access Selection

Requested Application

SCMS

Original Requested Roles

General Base Support (Required)

Requested Roles *

General Base Support (Required)



< Previous

Return Later

Cancel Request

Next >





SCMS SAAR

- Read the Acceptable Use Policy, click the **Accept** button to confirm, and click **Next** to move to the next step.

Complete Work Item

System Authorization Access Request (SAAR) - User Request

AUTHORIZED Acceptable Use Policy

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept

I have read and understand the Acceptable Use Policy. *

☒ Accept

○○○●○

< Previous

Return Later

Cancel Request

Next >



SCMS SAAR

- Enter a justification statement (required) in the **Justification For Access** text box. The justification reason may vary from organization to organization.
- Click **Next** to move to the next step.

System Authorization Access Request (SAAR) - User Request

JUSTIFICATION FOR ACCESS *

I am a SCIP analyst and require SCMS access for testing and troubleshooting.

*NOTE - Required Attachments Are:



◀ Previous

Return Later

Cancel Request

Next >





SCMS SAAR

- Select values for each of the dropdowns. You can select “All” values for **Country**, **Implementing Agency**, and **Country Service**. For **Country Groups**, if selecting multiple, you must select each country group individually. **NOTE** – If you are a foreign national, you may only select one country.
- Click **Submit** to move to the final step.

Complete Work Item

Request on Behalf: System Authorization Access Request (SAAR) - User Request

SCMS-Base

Country *

Implementingagency *

Countryservice *

Countrygroups *

Usertype *



◀ Previous

Return Later

Cancel Request

Submit





- Review the CAC Digital Signature Required statement.
- Click **I Acknowledge** to complete the submission process and move your request to the approvals process.
- **NOTE** – After clicking **I acknowledge**, it may take several seconds to return to the E-ICAM home screen.

CAC Digital Signature Required

By digitally signing this document with your Common Access Card (CAC), you are verifying access to U.S. Government (USG) Information Systems (IS). To the best of your knowledge, any decisions, statements, and/or comments provided within the System Authorization Access Request (SAAR) are accurate. You agree that your digital signature is the legally binding equivalent to your handwritten signature. Your digitally signed actions may be used as evidence including but not limited to court cases, court supervised mediation, third party mediation, firing procedures, quarterly audits, yearly audits, extraordinary review from third party observers, job performance reviews, internal audits, and operation evaluations.

This Digital Signature uses x509 certificate authentication.

You will be redirected to the Global Directory x509 login to complete the signature.

Cancel

I Acknowledge





DEFENSE SECURITY
COOPERATION AGENCY

Security Through Global Partnerships

