



WebRoR ICAM registration

Presented by:

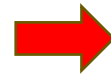
N52311 – Policy & Systems

August 6th 2026



WebRoR SAAR

- Go to Sailpoint to start process:
<https://spnfm01-acc.icam.disa.mil/identityiq/home.jsf>
- Click the 3 lines to expand the left-side menu



DoD E-ICAM 26-07 PRD

Notice: Upcoming changes with R26-08 will impact in-flight Access Requests. If not fully approved by 1600hrs ET 26AUG2026, open Access Requests will be cancelled. Impacted Access Request(s) will need to be resubmitted after the cancellation window closes at 2359hrs ET. Reference CHGU0231018 for ASI updates.

DISA

Home My Work ▾ ? 🔔 Bintner, Jessica ... ▾ Logout

Home Edit

Manage My Access > Track My Requests >

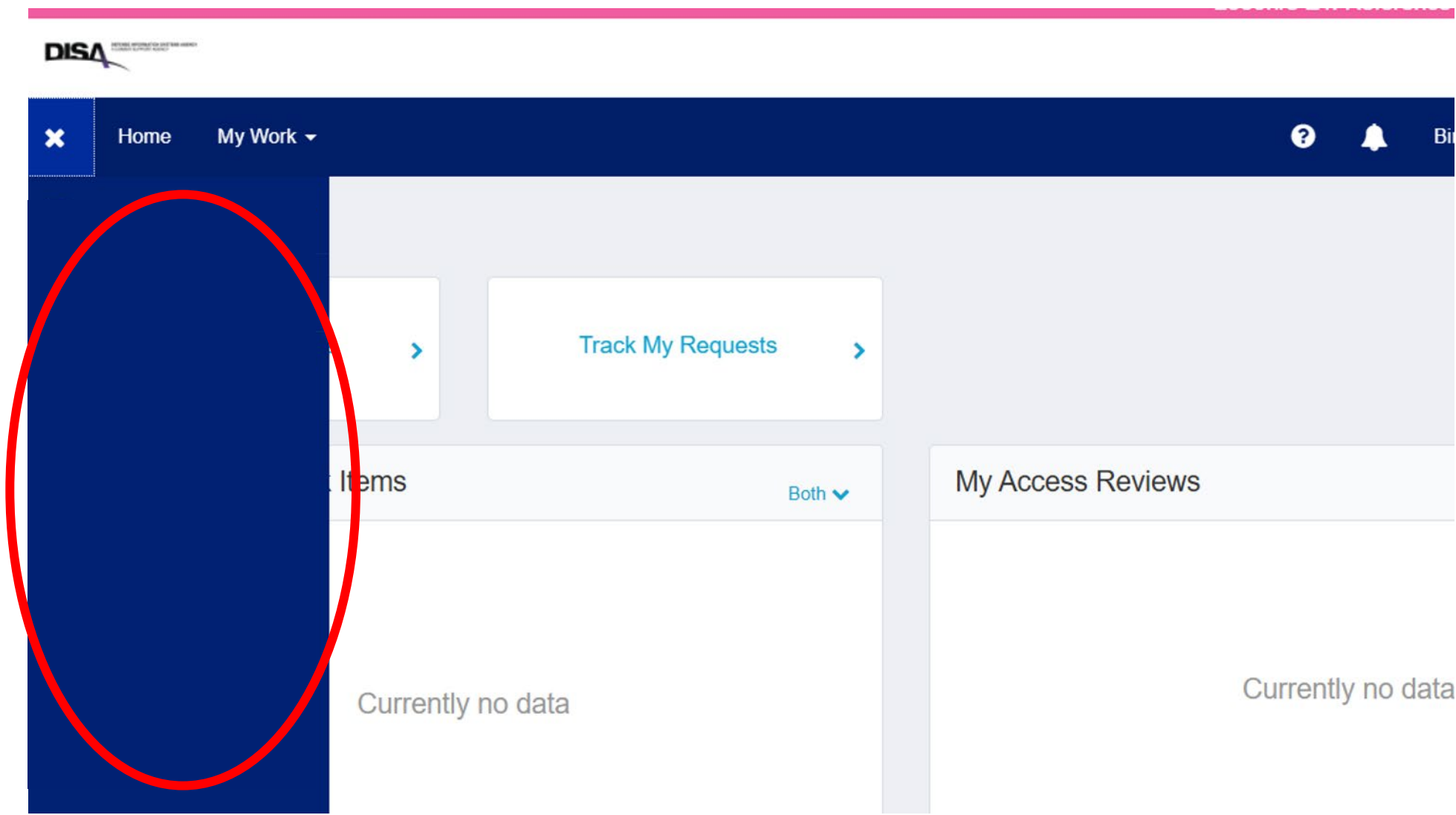
Latest Violation Work Items Both ▾

Currently no data

My Access Reviews

Currently no data

- If the menu is blank, please close all open internet browsers and reopen Sailpoint.
- If options appear in this menu, then please continue to the next slide.



WebRoR SAAR

- Click manage user access



WebRoR SAAR

- To narrow the list of roles, enter **WebRoR** in the Search bar and click the magnifying glass or press **Enter**

The screenshot displays the DISA WebRoR SAAR interface. At the top, there is a pink header bar. Below it, the DISA logo is visible. A dark blue navigation bar contains a menu icon, 'Home', 'My Work' with a dropdown arrow, a help icon, a notification bell, and the user name 'Bintner, Je'. The main content area is titled 'Manage My Access'. It features two steps: '1 Manage My Access' (Select access you would like to add or remove.) and '2 Review and Submit' (Look over your selections and confirm.). Below the steps, there are two tabs: 'Add Access' and 'Remove Access'. The 'Add Access' tab is active. A search bar is present with the text 'WebRoR' and a magnifying glass icon. A red arrow points to the search bar, and another red arrow points to the magnifying glass icon. To the right of the search bar is a 'Filters' dropdown menu. At the bottom, it says 'Showing 1-12 of 100'.



- Click the checkmarks to select **one user role** and **one user type**. The check mark will display as green when selected.
- User Type Options:
 - User type: Civilian
 - User type: Contractor
 - User type: Foreign National
- User Role Options:
 - User role: Read Only
 - User role: Customer
 - User role: Repair Manager
 - User role: Depot User
- **Note:** DoD E-ICAM prevents you from selecting multiple roles within the same SAAR.

☒	WebRoR User Type Civilian			
Type: Role	Access Type: AUTHORIZED	Appointment Letter: f	Authorization Letter: f	Privileged User Agreement: f

☒	WebRoR User Role Repair Manager			
Type: Role	Access Type: AUTHORIZED	Appointment Letter: f	Authorization Letter: f	Privileged User Agreement: f

Caution: Make sure WebRoR is selected, not WebRoR Dev or WebRoR Test.

The following icons are located to the right of each access:

- Paperclip for uploading attachments
 - For roles requiring uploaded documentation, this icon will be marked with a **RED** asterisk.
- Speech button for entering comments
- “Details” for showing additional details, if applicable.

Click the paperclip icon with the **RED** asterisk to upload your cyber security certificate (PDF only).

Identities Selected: Chaouch, Jenna M CIV USN NAVSUP WSS PHIL (USA)

Normal

Add Access 2

WebRoR User Role Repair Manager

Details

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

WebRoR User Type Civilian

*

Details

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

Previous

Cancel

Submit

WebRoR SAAR

- Drag-and-drop a supporting file 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:** The Supervisor is responsible for verifying the attached files; DoD E-ICAM does not validate PDF content. All uploaded files are attached to the Supervisor's email notification for the request.

Attach a File to WebRoR User Type Civilian

Drag and drop file here

Or click to upload a file

Attached to This Item

JBintner Oct 2025 Cyber Awareness Challenge Certificate.pdf

Enter a description

Role:

Access Type: AUTHORIZED

Appointing Letter: 1

Authorization Letter: 1

Privileged User Agreement: 1

Identities Selected: Chaouch, Jenna M CIV USN NAVSUP WSS PHIL (USA) Normal

Add Access 2

✕ WebRoR User Role Repair Manager

Details

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

✕ WebRoR User Type Civilian

Details

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

Previous

Cancel

Submit

- Click **Submit**

WebRoR SAAR

- Click **Complete Form**.

Home My Work Intelligence ? Chaouch, Jenna ... Logout

More Info Needed

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

Identity: Chaouch, Jenna M CIV USN NAVSUP WSS PHIL (USA)

Later **Complete Form**

WebRoR

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

WebRoR User Type Civilian 1 Details

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

Previous Cancel Submit

© Copyright 2023 SailPoint Technologies - All rights reserved. | Powered by SailPoint IdentityIQ

- Review the Privacy Act Statement screen and click **Next**.



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 >

Complete or review the following fields (required fields are indicated by a red asterisk on the form; some fields are pre-populated):

- Type of Request** – Initial or Modification. The system pre-selects **Initial**. You should only adjust to **modification** if you have already submitted a SAAR within Sailpoint for WebRoR.

- Supervisor Email**

NOTE: If the Supervisor information is not auto-populated, then enter your supervisor’s email address in this field. If the email address is found in the database, then the system auto-populates the **Supervisor Name** field.

- Click **Next**.

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	SYSTEM LOCATION + (Location of system)	TYPE OF ACCESS REQUIRED: * AUTHORIZED
NAME * Chaouch, Jenna M CIV USN NAVSUP WSS F	ORGANIZATION * USN	OFFICE SYMBOL/DEPARTMENT * NAVSUP WSS PHIL
PHONE (215) 697-3771 If phone cannot be validated please select None.	OFFICIAL EMAIL ADDRESS * jenna.m.chaouch.civ@us.navy.mil	JOB TITLE AND GRADE/RANK * Logistics Manager
OFFICIAL MAILING ADDRESS * Philadelphia, PA (incl. all Federal sites)	CITIZENSHIP * US	DESIGNATION OF PERSON * CIV
ACCESS EXPIRATION DATE mm/dd/yyyy	SUPERVISOR EMAIL * charles.a.pinnelli.civ@us.navy.mil (Supervisor Email search)	
SUPERVISOR NAME * Pinnelli, Charles A CIV USN NAVSUP W		

3 Review

Look over

WebRoR SAAR

- Review the access selection and click **Next**.

Work Intelligence

Complete Work Item

System Authorization Access Request (SAAR) - User Request

Access Selection

Requested Application

WEBROR

Original Requested Roles

WebRoR User Type Civilian

WebRoR User Role Repair Manager

Requested Roles *

WebRoR User Type Civilian

WebRoR User Role Repair Manager

Progress: 00●000

[Previous](#) [Return Later](#) [Cancel Request](#) [Next >](#)

WebRoR SAAR

- Read the Acceptable Use Policy, and then select **Accept** to confirm.
- Click **Next**.

work Intelligence

Complete Work Item

System Authorization Access Request (SAAR) - User Request

AUTHORIZED Acceptable Use Policy

protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

I have read and understand the Acceptable Use Policy. *

☒ Accept

○○○●○○

[< Previous](#) [Return Later](#) [Cancel Request](#) [Next >](#)

ess type. AUTHORIZED Appointment Letter. Authorization Letter. Privileged User Agreement.

User Type Civilian



- Enter a justification statement in the **Justification for Access** text box.
- Prior SCIP Users: Please provide your SCIP User ID (if known).

***NOTE:** Justification for Access is required for approval. The content required in the justification may be different for each organization or system.

- Click **Next**.

The screenshot shows a web application interface for completing a work item. The title bar reads "Complete Work Item". Below it, the subtitle is "System Authorization Access Request (SAAR) - User Request". A section titled "JUSTIFICATION FOR ACCESS *" contains a text area with the text "I am a repair manager I need WebRoR access to track repair and return." A red arrow points to this text area. Below the text area, a note states "*NOTE - Required Attachments Are:". Underneath this note is a list of attachments, including "Cyber Awareness completion certificate". At the bottom of the form, there are navigation buttons: "< Previous", "Return Later", "Cancel Request", and "Next >". A red arrow points to the "Next >" button. The footer of the page displays status information: "Access Type: AUTHORIZED", "Appointment Letter: f", "Authorization Letter: f", and "Privileged User Agreement: f".

WebRoR SAAR

- Complete the selections for all extended (additional) attributes. Required fields are indicated with a red asterisk.
- Click **Submit**. Upon submission, DoD E-ICAM sends an email notification to the Supervisor with all attachments and selected roles.

Complete Work Item

System Authorization Access Request (SAAR) - User Request

WEBROR-User_CIV

Implementingagency *

Navy

Customerservicedesignator *

Navy

Country *

All

Pseudocountry *

None

Repairgroup *

NAVSUP Aviation

Progress indicator: 6 circles, 5th circle filled.

Buttons: Previous, Return Later, Cancel Request, Submit

WebRoR SAAR

- Review the **CAC Digital Signature Required** message.
- Click **I Acknowledge**.

Comments can be left blank

Complete Work Item

Digital Signature

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.

Comments

NOTE: All rejected access requests require an explanation in the comments field.

I Acknowledge



Supervisor Approvals

WebRoR SAAR- Supervisor Approvals

DoD E-ICAM sends an email notification to the Supervisor

1. From the home dashboard, click **My Work > Work Items**.
2. Click **View** to begin reviewing the system access request.
3. Review the Privacy Act Statement and click **Next**.
4. Review the requestor's information and verify that it is accurate.
5. Click **Next**.
6. Specify the Security Manager:

NAVSUP Security POCs:

joseph.e.stives.civ@us.navy.mil

jarett.r.kubeck.civ@us.navy.mil

AFSAC Security POC:

maria.powers.1@us.af.mil

USASAC Security POC:

george.e.lawrence3.civ@army.mil

7. Click **Next**.

System Authorization Access Request (SAAR) - Supervisor

1 Download

How to fill out the Security Manager information

OPTION 1: Enter the Security Manager Email directly.

OPTION 2: Expand the Security Manager Name drop-down and select an individual or workgroup.

NOTE: If an email was already entered in the Security Manager Email field, that field must be cleared first before selecting a workgroup.

OPTION 3: Leave both of the Security Manager fields blank. DoD E-ICAM automatically assigns the SAAR to the security manager workgroup based on the requestor's organization and location values. Leave both of the Security Manager fields blank. DoD E-ICAM automatically assigns the SAAR to the default or custom security manager workgroup based on the requestor's organization and location values.

More Info: <https://dod365.sharepoint-mil.us/sites/DISA-ICAM/SitePages/Approving-User-Access.aspx>

SECURITY MANAGER EMAIL	SECURITY MANAGER NAME
(Security Manager Email search)	(Security Manager Name search)

Previous
Return Later
Reject

Next

WebRoR SAAR- Supervisor Approvals

8. Review the selected roles and associated attributes

9. Click **Next**.

10. Review the Justification for Access.

11. If not already populated, then select an **IA Training and Awareness Certification Requirements** date from the date picker.

****NOTE** -The Supervisor must verify the content of the PDF attachment(s) as the DoD E-ICAM system does not validate the contents of attachments.

12. Select the **Verification of Need-to-Know** radio button to certify that the requestor requires the access as requested.

13. Select the **User Requires Access To** value from the drop-down list. Single or multiple values can be selected.

System Authorization Access Request (SAAR) - Supervisor

1 Download

JUSTIFICATION FOR ACCESS *

Access required to perform my duties as the WebRoR Delivery Manager

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *

mm/dd/yyyy

This field is required

I have verified the submitting user has completed their Annual Information Awareness Training on the date listed above.

VERIFICATION OF NEED TO KNOW *

☐ Select to certify that this user requires access, as requested.

This field is required

USER REQUIRES ACCESS TO *

This field is required

ACCESS EXPIRATION DATE

mm/dd/yyyy

Progress: 000001

Previous

Return Later

Reject

Next

WebRoR SAAR- Contractor User Type

14. Select an **Expiration Date** from the date picker if the user has not already entered this information.

Caution: The Contract/Access Expiration Date cannot be in the past, but it can be set to any future date.

Note: For contractor personnel, the Expiration Date field will say **Contract Access Expiration Date**. For CIV and military personnel, the field will say **Access Expiration Date**.

15. Verify that the **Company Name** is populated in the field.

16. Verify that the **Contract Number** is populated in the field (contractor personnel only).

17. Click **Next**.

18. Click **Approve**.

Note: If the field is empty and displays a red asterisk, then the Supervisor must complete it.

The screenshot shows a web form for contractor user type. It includes several required fields marked with red asterisks: 'VERIFICATION OF NEED TO KNOW', 'CONTRACT ACCESS EXPIRATION DATE', 'CONTRACT NUMBER', 'USER REQUIRES ACCESS TO', and 'COMPANY NAME'. The 'VERIFICATION' field has a radio button selected. The 'EXPIRATION DATE' field shows '05/25/2025' with a calendar icon. The 'CONTRACT NUMBER' field shows '12345'. The 'ACCESS TO' dropdown is set to 'Unclassified'. The 'COMPANY NAME' field shows 'New Company Name'. At the bottom, there are navigation buttons: '< Previous', 'Return Later', 'Reject', and 'Next >'. A progress indicator shows four circles, with the third one filled.

VERIFICATION OF NEED TO KNOW *

☒ Select to certify that this user requires access, as requested.

CONTRACT ACCESS EXPIRATION DATE *

05/25/2025

CONTRACT NUMBER *

12345

USER REQUIRES ACCESS TO *

Unclassified

COMPANY NAME *

New Company Name

000●0

< Previous Return Later Reject Next >

WebRoR SAAR- Supervisor Approvals

20. Review the **Digital Signature** message.

21. Enter any relevant comments, if applicable, in the Comments field, and then click **I Acknowledge**.

Digital Signature

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.

Comments

I Acknowledge



WebRoR SAAR

For any additional questions or support, please contact:

Jenna Chaouch, Program Manager: jenna.m.chaouch.civ@us.navy.mil

Steven Morris, Operations Manager: steven.m.morris39.civ@us.navy.mil

Tim Anderson, Delivery Manager: timothy.r.anderson96.civ@us.navy.mil