Transcript: How to submit a SAAR Form a New/Renew Account by NON-DCMA USG Employee Training Video

Slide 1

PDREP Product Data Reporting and Evaluation Program –
How to submit a System Authorization Access Request (SAAR) Form for a new/renew account by Non-DCMA USG Employee Training Video

Slide 2

Agenda for general access is

1. Link to PDREP
2. General attributes of a US Gov't user
3. Checklist: things needed to get started
4. Type of request new/renew
5. Confirm that I AM A: USG Employee.

Slide 3

Agenda for User Access Request Process is

1. User Information Block
2. Data Required Section
3. Confirm Citizenship, Information Assurance Training
4. Justification for Access, User agreement
5. Sign and Submit.

Begin demonstration video.

On screen: Image of PDREP website home page.

Welcome to the Product Data Reporting and Evaluation Program - Automated Information System (PDREP-AIS) Training Videos.

This video explains how to submit a System Authorization Access Request (SAAR) Form for a new account or to renew a deactivated account by a Non-DCMA USG Employee.

This video applies only to personnel that are NOT DCMA employees. There is a separate training video for their unique DCMA SAAR requirements.

USG employees issued a Common Access Card (CAC) may request access to PDREP-AIS. Access privileges are dependent on their Agency, Service, and Service Command, affiliation with the DOD and/or local activity's agreements with the PDREP-AIS.

All DOD employees (military and civilian) and non-DOD Contractors (private industry partners) are required to use a valid DoD PKI Certificate to access the PDREP-AIS in accordance with DOD Instruction 8520.02.

First time PDREP-AIS requesters and users with deactivated accounts will need to submit a SAAR-P (NEW/RENEW respectively) from the PDREP-AIS home page

To Submit a SAAR, using the web browser of your choice, go to https://www.pdrep.csd.disa.mil (It is recommended that users work with Microsoft Edge or Google Chrome.)

NOTE: Microsoft Internet Explorer is obsolete and should not be used.

Here you will need click the link labeled “Request Access”, the browser will navigate to the PDREP-AIS Account Type Definitions web page.

On screen: Click on Request Access button in top menu. PDREP Account Type Definitions Request Access page opens.

As a reminder, this training video is for **US Government Access Non DCMA users General Attributes of a US Government User are:**

- You are a military or civilian personnel working for the U.S. Government.
- You have been issued a USG Common Access Card (CAC) without a green or blue stripe.
- You have a verifiable need to access various USG information systems (IS) to complete work as directed by your service/component.
- You may receive access to information as required or directed by your service/component.

Once you have ensured that you fall under the category for US Government Access, select the link, “LINK TO WHAT DO I NEED BEFORE I GET STARTED (GOVERNMENT)”. Requesters will be navigated to the ‘What do I need before I Get Started’ page.

On screen: What do I need before I “Get Started”, Government Employee page.

Where a checklist will be found.

- CAC without stripe
- Your name
- Your work location DoDAAC
- Your Phone Number
- Your email
- Your supervisor email and
- Your security manager email. (There is a cybersecurity requirement to include your Security Manager information when submitting a SAAR-P for user access

IMPORTANT: The NSLC Portsmouth Help Desk will NOT know who your organization's Security Manager is. Please, go through your Chain of Command to determine your Security Manager's information.

Once requestor has all required information user can select Start Government Access Request. At this point you may be asked to select a certificate. Select appropriate certificate. Requester will be navigated to the SAAR-P with User type Pre-populated.

On screen: SAAR-P form

First you will verify the type of request.

New- from dropdown menu

- Requester has never had a PDREP-AIS account.

- Requester is reapplying but is switching between the five different account types (USG to CTR or CTR to USG).
- Requester is reapplying but is changing component (i.e. USN to USA).

Renew- from dropdown menu

- User account was deactivated because they did not login in the past 30 days.
- User account was deactivated because contract had expired and replace or extended contract is in place.

Confirm that I AM A: USG Employee is selected here.

Then complete 'User Information' block

1. Last Name (Mandatory). Doe
2. First Name (Mandatory) and Middle Initial (Optional). Jane T
3. Primary DoDAAC (Mandatory) – Enter the Department of Defense Activity Address Code for the organization for which you primarily work. – N00391

   This auto fills the following information from PDREP data base. PDREP pulls this information from system of record, DLA's Defense Automatic Addressing System (DAAS). If this information is incorrect, user needs to contact source system, not PDREP, to have this information updated.
   - ✓ DOD Activity Name
   - ✓ Office Address
   - ✓ City
   - ✓ State
   - ✓ Zip Code
4. Additional DoDAAC (Optional) – If you perform work for multiple organizations, you may enter more than one DoDAAC. Requesters will need to justify additional DoDAACs that are not within the same component (i.e. NAVSUP and NAVSEA or DLA and Army).
5. Office Symbol/Department (Optional) for Non-DCMA.
6. Commercial Phone Number
   i. Area Code (Mandatory) - 207
   ii. Work Phone Number (Mandatory) - 438-1690
   iii. Extension (Optional)
7. DSN (Optional)
8. Fax (Optional)
9. International Phone Number (Optional)

Complete the 'DoD Data Required' Section

1. Gov't Email Address (Mandatory) – requester's e-mail address (i.e. first.last@mail.mil) but can be '.org' or '.gov' but not '.com'.
2. Gov't Supervisor Email Address (Mandatory) – requester's supervisors (or their representative) email address.
    - The Supervisor email cannot be same as requester's e-mail address.
3. Gov't Security Manager Email Address (Mandatory) - requestors Security manager. Please go through your Chain of Command to determine your Security Manager's information.

    If you know your security managers email, enter it. The Security Manger's information may be left blank by the Submitter; however, after the SAAR is submitted to their supervisor or USG sponsor, it is then mandatory to for the supervisor or USG sponsor to enter it and froward to their activities security manager. The SAAR-P must be sent to, and then verified by the organization's Security Manager. The Security Manager verifies your Background Investigation and Clearance levels.

On screen: Showing PDREP Reporting Tools and their optional sections available.

Select Accesses (Optional) - SAAR access level availability will vary, depending on type of account (USG or CTR) and components (ARMY or Navy) and business/process owner approval so requester's actual screen of accesses may vary. SAARs without any access requested will be processed as 'Search Only'. User guides for each module to assist in determining applicability can be found on PDREP Web Page and selecting 'References' then selecting 'Guides and Manuals'.

Please NOTE: Only select access that pertains to your duty and/or Agency. While you may ask for access to any module, be aware you will only receive access to the module dependent on your Agency, Service, Service Command, or local activity's agreements with the PDREPAIS and USG supervisor/sponsors approval. PDREP –AIS is For Official Use Only – Business Sensitive (FOUO-BS) so selections should be made on a need for access. Refer to users guides to applicability for each module.

1. Product Quality Deficiency Report - PQDR Application: Select the boxes for the access levels required.
2. Supply Discrepancy Reports – SDR Application: Select the boxes for the access levels required.
    i. Army, Air Force and DLA can only have View access.
    ii. The official SDR processing system for the Army is DLA's WebSDR.
    iii. DLA can only get SDR if their Primary DoDAAC is a Navy DoDAAc
3. RIMS/SAM/ERS NNPI –only select Nuclear User if you are authorized access to any of these modules and you work in the nuclear environment.
4. Receipt Inspection Management System (RIMS), (Navy Users Only).
    i. Select your user role from the drop down list.
    ii. Select CIM user only if Controlled Industrial Material pertains to you.
5. Supply Action Module (SAM), (Navy and NNPI Users Only). - Select your user role form the drop down list.
6. Corrective Action Request (CAR) - View Access Only for Non DCMA users.
7. Quality Assurance Letter of Instruction (QALIs) and Letters of Delegation (LODs) – View Access and non DCMA Originator for Non DCMA users.

8. Surveillance Plan (SP) - View Access Only for Non DCMA users
9. Engineering Referral System - ERS Application, (Navy and NNPI Users Only): Select the boxes for the access levels required.
10. Virtual Shelf (VSF) – is not being added to accounts at this time.
11. SPPI Bulletin (SB) – limited to Read only
12. SRS – is not being applied to accounts at this time.
13. Other PDREP Tools: Check the boxes that apply to your requirements.

Once the selections have been made Confirm Citizenship (Mandatory) and Information Assurance Training (Mandatory) an additional mandatory check box will appear if you selected the NNPI check box in the select accesses section above.

Note the Information Assurance Training is a DOD cybersecurity requirement and mandatory. If you have not completed or aren't sure you have completed it, you can complete the training at this URL: https://public.cyber.mil/training/cyber-awareness-challenge/. NOTE: PDREP-AIS does not hold or sponsor a class.

Next you will need to provide justification for Access this is a Mandatory field. The justification will be included in the email sent to your supervisor.

In order to proceed select Click to read the agreement the user agreement appears in a pop up window.

On screen: User Agreement popup window.

Read and scroll through the user agreement. At the end of the user agreement either select "I have read the agreement and agree to follow" which will navigate the browser back to the SAAR-P with a sign and submit button or "I do not agree" Which will navigate the browser back to the previous screen where it will ask you to select Click to read the agreement this is a Mandatory field.

On screen: SAAR-P showing the Sign and Submit button.

Select the 'Sign and Submit Request' button. After selecting the 'Sign and Submit Request' button, user will receive a confirmation). The PDREP ID is not your User ID. This is the serial number of the SAAR-P for tracking purposes. If you do not see this confirmation, your SAAR-P was not submitted successfully.

Please NOTE: Requester is DIGITALLY SIGNING affirmation to the User Agreement and SAAR-P is stamped with user information from CAC/Cert.

On screen: SAAR-P affirmation window with PDREP ID number, stating request has been submitted.

A confirmation e-mail, stating PDREP has received the SAAR-P submission and that a notification has been sent to the supervisor for approval will be sent to the requesters e-mail as listed on the SAAR-P.

This completes the training video on how to submit a SAAR Form for a New/Renew request being submitted by a Non DCMA USG Employee.

Slide Things to Note:

Additional DoDAAC

1. If you perform work for multiple organizations, you may enter more than one DoDAAC.
2. Requestors will need to justify additional DoDAACs that are not within the same component (i.e. NAVSUP and NAVSEA or DLA and Army).

Correct Emails

1. Make sure the US Government Supervisor's e-mail address is correct. Your Supervisor will receive a notice about your access request and is required to certify the need and authorization for access.
2. The Supervisor and Security Manager Email cannot be changed, only deleted, and requestor will have to resubmit if e-mail address is invalid.

IAT Link

1. Link to Information Assurance Training (IAT)
2. https://public.cyber.mil/training/cyber-awareness-challenge/

End Slide

Thank you for watching: How to Submit a System Authorization Access Request (SAAR) Form for a New/Renew account by a Non DCMA USG Employee Training Video.