Transcript: How to submit a SAAR Form a New/Renew Account by 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 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 DCMA USG Employee.

This video applies only to personnel that are DCMA employees. There is a separate training video for their unique to Non-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 DCMA users only:**

General attributes of a user:

- 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 where a checklist will be found.

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

- CAC without stripe
- Your name
- Your work location DoDAAC
- Your Phone Number
- Your email
- Your supervisor’s email and
- Your security manager’s 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. Requestor will be navigated to the SAAR-P with User type Pre-populated.

On screen: SAAR-P form

Here 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). - entered Doe
2. First Name (Mandatory) and Middle Initial (Optional). – entered Jane T
3. Primary DoDAAC (Mandatory) – Enter the Department of Defense Activity Address Code for the organization for which you primarily work. – entered S0512A

   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
   - ✓ Operational Unit (Region) (Mandatory) – select a unit from the drop down list. This will pre-populate the corresponding list in the Team Code drop down list.
   - ✓ Team Code – select your team code from the drop down list. This will update the SAAR-P and add a supervisor field.
   - ✓ Team Supervisor – select your team supervisor from the drop down list. This will pre-populate your supervisors email in the DoD Data Required block.
   - ✓ Job Series/Title - select applicable item from drop down list.

   NOTE: There may be several supervisors or there may be no supervisors or your supervisor may not be on the list. This list is provided by DCMA-HQ. If your supervisor is not listed, please contact the NSLC Help Desk.

4. Additional DoDAAC (Optional) – If you perform work for multiple organizations, you may enter more than one DoDAAC. Requestors will need to justify additional DoDAACs that are not within the same component (i.e. NAVSUP and NAVSEA or DLA and Army).
5. Commercial Phone Number
   a. Area Code (Mandatory)
   b. Work Phone Number (Mandatory)
   c. Extension (Optional)
6. DSN (Optional)
7. Fax (Optional)
8. International Phone Number – (Optional)

Complete the ‘DoD Data Required’ Section

1. Gov’t submitter 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.
    - For DCMA, this is prepopulated by selecting Supervisor from drop down list. If you are the team supervisor, your email address is prepopulated and you need to change this to your supervisor’s email.
3. Gov’t Security Manager Email Address (Mandatory) - 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 forward 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) - 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 PDREP-AIS 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.
    - Management level access may be provided if the DCMA person’s status as a DRPM is verified. Personnel that are not DRPMs, but QARs, should request Non-Management Support Point level access.
2. Supply Discrepancy Reports – SDR Application: Select the boxes for the access levels required.
    - SDR support is not being applied to accounts at this time.
3. Corrective Action Request (CAR), Quality Assurance Letter of Instruction (QALIs) and Letters of Delegation (LODs) and Surveillance Plan (SP) - Any access level, except “Non-DCMA View Access” is permitted if requested and approved by Supervisor/USG Sponsor and Security Manager on the submitted SAAR and may be processed by the PDREP Administrator.
4. Virtual Shelf (VSF) - is not being added to accounts at this time.
5. SPPI Bulletin – limited to Read only.
6. SRS – is not being added to accounts at this time.
7. 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)

Note the Information Assurance Training is a DOD cybersecurity requirement. 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/sponsor a class.

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

In order to proceed select Click to read the agreement (Mandatory) 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 as 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

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 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. Requesters 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 requester 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 DCMA USG Employee Training Video.