



User Access Request and Login Procedures

User Guide
29 January 2025

Table of Contents

FOREWORD	3
REFERENCES	3
INTRODUCTION	5
1 TYPES OF USER ACCESS	7
1.1 User Types.....	7
1.2 Access Levels	9
2 OVERVIEW OF USER ACCESS REQUEST PROCESS	10
3 ACCESSING THE SAAR-P	12
3.1 Users without Active Accounts.....	12
3.2 Users with Active Accounts	18
3.3 BETA Users without Active Accounts	19
3.4 BETA Users with Active Accounts.....	19
4 COMPLETING THE SAAR-P (SUBMITTER)	20
4.1 Review Request Type.....	20
4.2 User Information	21
4.3 User information – Additional DCMA Fields.....	23
4.4 DoD Contractor Data Required (Contractors Only).....	25
4.5 DoD Data Required.....	27
4.6 Request Access Levels	29
4.7 Citizenship and Training Confirmations (Mandatory) (See Figure 4.13).....	33
4.8 Justification for Access (Mandatory) (See Figure 4.14)	33
4.9 Read and Agree to User Agreement.....	34
4.10 Sign and Submit SAAR-P	35
5 APPROVING THE SAAR-P (SUPERVISOR/SPONSOR)	36
5.1 Accessing SAAR-P	36
5.2 Validating SAAR-P.....	39
5.3 Certifying User/Self Type and Contract Information.....	42
5.4 Approving or Disapproving SAAR-P	44
6 VERIFYING SUBMITTER BACKGROUND (SECURITY MANAGER)	45

6.1	Accessing SAAR-P	45
6.2	Enter Background Information.....	48
6.3	Verifying or Rejecting SAAR-P.....	50
7	PROCESSING THE SAAR-P (PDREP ADMIN)	51
8	PDREP LOGIN	52
8.1	Initial Login (Synchronizing Account with CAC/PIV/Cert)	52
8.2	Follow-on Login.....	60
8.3	Login Failures.....	63
9	PDREP HELP	65
10	USER PROFILE	66
10.1	Viewing Your User Profile.....	67
10.2	Editing Your User Profile.....	68
10.3	Creating and Editing Distribution Lists.....	70
10.4	Creating and Editing Point of Contact (POC).....	75
10.5	Submitting an Access Change Request.....	81
.11	ACCOUNT DEACTIVATION	83
11.1	Active Accounts	83
11.2	Disabled Accounts.....	83
11.3	Deactivated Accounts.....	83
11.4	End of Contract	83
11.5	Deactivation Requests	84
12	ADMINISTRATIVE ACCOUNT ISSUES	85
12.1	New CAC/PKI Cert.....	85
12.2	E-Mail Change	85
12.3	Supervisor Change	85
13	SUMMARY	86
	APPENDIX 1 – NOTIFICATIONS	87

*Hold the 'CTRL' key and click on paragraph to follow link

FOREWORD

This user guide provides information about the Product Data Reporting and Evaluation Program - Automated Information System (PDREP-AIS) and is intended to assist users with the User Access module functionality. This document does not cover specific policy or procedure and is designed to work in concurrence with existing processes. This guide does not replace or amend any Department of Defense (DoD) instructions, regulations, and/or policies. Revisions to this guide are made after application changes have been implemented. Date of last amendment is located on the title page. Though this document is accessible to all users, its content is intended for those individuals with module access. Module access is granted on a case by case and need to know basis.

NOTE: The data contained within this guide is NOT real data and it is NOT to be used for business purposes. The material presented is intended to serve as an example only and was taken from a test system.

REFERENCES

- Department of Defense Warranty Guide, V2.0
- DFARS 246.7
Defense Federal Acquisition Regulation Supplement 246.704, Authority for use of warranties
- DLAR 4155.24
Product Quality Deficiency Report Program
- DoD Instruction 5000.2
Operation of the Defense Acquisition System
- DoD Instruction 5000.79
Defense-Wide Sharing and Use of Supplier and Product Performance Information (PI)
- DoD Instruction 5200.48
Controlled Unclassified Information (CUI)
- FAR 46.7
Federal Acquisition Regulation 46.7, Warranties
- NAVSO P3683
Navy Standard Operating Procedure 3683 (NAVSO P-3383), Navy and Marine Corps Product Data Reporting and Evaluation Program
- NAVFAC 4855.1

Naval Facilities Engineering Command Instruction 4855.1, Product Data Reporting and Evaluation Program

- NAVSEA 4855.39

Naval Sea Systems Command Instruction 4855.39, Implementation of the Product Data Reporting and Evaluation Program

- SECNAV Instruction 4855.3

Secretary of the Navy Instruction 4855.3, Product Data Reporting and Evaluation Program

- SECNAV Instruction 4855.5

Secretary of the Navy Instruction 4855.5, Product Quality Deficiency Report Program

- SPAWAR 4440.12A

Space and Naval Warfare Systems Command Instruction 4440.12, Management of Operating Materials and Supplies, Government Furnished Property, and Inventory

INTRODUCTION

This document is intended to guide personnel in the use of Product Data Reporting and Evaluation Program – Automated Information System (PDREP-AIS) User Access module.

The PDREP-AIS is accessible via the Product Data Reporting and Evaluation Program home page: <https://www.pdrep.csd.disa.mil/>

Getting Access

- **First Time Users**

First time users are required to submit an on-line PDREP-AIS System Authorization Access Request (SAAR) form. Instructions are available on the PDREP home page as linked above. Click on the [Request Access](#) link for instructions on filling out an access request form. When requesting an account, ensure all fields indicated as mandatory are completely filled out. Mandatory fields are indicated by (M). The application will not be accepted if required information is missing.

- **Existing PDREP Users**

Existing PDREP users may request additional or updated access privileges by submitting an updated SAAR. To do this, log into the PDREP-AIS and hover over your name in the upper right corner of the page and select 'Access Change Request'. Update the SAAR and enter a narrative to describe requested changes, read and acknowledge the User Agreement and click 'Sign and Submit Account Change Request' button to complete the submission.

Contact us

Contact us by submitting a help desk ticket either via the "Contact Help Desk" button in the lower right corner of our PDREP website or via the "Help" menu within the PDREP-AIS Application.

Additional Resources available on the NSLC Portsmouth Homepage

In order to aid PDREP-AIS users, reference these additional resources as needed:

- [FAQ](#) – On the PDREP website under References, the Frequently Asked Questions page gives quick answers to the most commonly received inquiries. Your question(s) may be easily answered there.
- [Guides & Manuals](#) – This area of the PDREP website (under References) houses the PDREP-AIS' technical documents. These comprehensive guides serve to offer directive on operational tasks and enable users to pinpoint or problem solve without expert assistance. These manuals do not instruct on policy or process and are instead stepwise instructions on using the PDREP-AIS application. Relevant process and policy are however referenced in the beginning of each of these manuals.
- [Online Training](#) – Computer-based distance learning may be accessed through the Reference fly-out of the PDREP website. Instruction takes place remotely via instructor-led directive, module simulation, video-conferencing, application demonstration, or recorded lesson.

FAQ, User Guides and Online Training are also accessible within PDREP-AIS by hovering over the 'Help' link located at the top left of each application page.

1 TYPES OF USER ACCESS

1.1 User Types

Access to the functionality of the USER ACCESS application is determined by the User's Access Level. PDREP-AIS has several Access Types for the System Authorization and Access Request - PDREP-AIS (SAAR-P) application.

There are four general types of personnel that may request access to the PDREP-AIS. These type of accounts are US Government employee (Military or Civilian) and three types of contractors: Support Contractor, Prime Contractor and Tier 2 Subcontractor (See **Table 1.1**).

All PDREP-AIS users are required to use a valid DoD PKI Certificate to access the PDREP-AIS in accordance with DOD Instruction 8520.02.

Table 1.1: User Types

User Type	Functions
USG Employee	Any USG employee (Military or Civilian) may request access to the PDREP-AIS. Access privileges are dependent on their Agency, Service, Service Command, or local activity's agreements with the PDREP-AIS.
USG Support Contractor	USG Support Contractors act as an agent of the government as if they were a government employee. Their contract is a Personal Services type contract (FAR 37.104) which characterizes the employer-employee relationship it creates between the Government and the contractor's personnel. USG Support Contractors are issued a USG Common Access Cards (CAC)/Personal Identity Verification (PIV) and have non-disclosure agreement. They may apply for access in a similar manner as USG employees with CACs. The US Gov't Supervisor certifies the need for access to the PDREP-AIS and that the purpose is to perform the duties assigned by the US Government are in accordance with their company's USG contract. This level of access can permit access to process data as required and limited by the companies USG contract.
Prime Contractor	Prime Contractors act as an agent of their company. Their access is limited to records as they pertain to only their company (DoDAAC/CAGE).

<u>User Type</u>	<u>Functions</u>
	<p>Personnel working for a company that have current contracts with the USG and are required to process data with the USG in order to fulfill their contractual obligations are considered Prime Contractors. Persons, authorized by the company and with a USG sponsors certification/approval, may receive access to view their company's data, by CAGE and/or Contracted DoDAAC to work data as required by the contract in the PDREP-AIS. The Prime Contractor's company must be registered in System for Award Management (SAM) and have a CAGE(s) code. The contractor must be sponsored by the USG. The USG sponsor verifies the person works for the company, a valid contract exists, and the contract has not expired. This level of access only permits access to the company's information in the PDREP-AIS and is restricted from viewing any other company's data.</p>
<p>Tier 2 Subcontractor</p>	<p>Tier 2 Subcontractors work for companies that do not have a contract with the US Government for the scenario for which they are applying for PDREP-AIS access.</p> <p>They do have a signed subcontract/MOU/MOA with a company that does have a signed contract with the US Government. Depending on the Tier 1 company's contract, the Tier 2 Subcontractor may be treated either as a Support Contractor or a Prime Contractor.</p>

1.2 Access Levels

Access to PDREP-AIS records depends on levels requested on the SAAR-P (See **Table 1.2**). Some record types will have Drop Down Lists (DDLs) and permissions for those record types are set by module and selection from the DDL. Other modules will have check boxes for access. For PQDR, SDR, MIR, SAA, SSR, SQD, SRV, TST and CAD modules, the checkbox will request non-management access. If user requires access for all records for a record type for their activities, they need to identify that requirement by stating they need MANAGEMENT ACCESS for that record type in the JUSTIFICATION field on the SAAR-P.

Table 2.1: Access Levels

<u>Access Level</u>	<u>Access Permissions</u>
No Access	User may not access or view record type.
Non-Management Access	Users may view and create records in specific record type. Users may only update records that they created.
Management Access	Users may view and create records in specific record type. Users may update all records at their approved activities (DoDAACs).
Full Access	Reserved for PDREP-AIS admins.

2 OVERVIEW OF USER ACCESS REQUEST PROCESS

- Submitter submits a System Authorization Access Request-PDREP (SAAR-P) to request access.
- Submitter is notified that PDREP-AIS has received the SAAR-P and a notification has been sent to the approver (Supervisor/Sponsor) as listed on the SAAR-P.
- Approver (Supervisor/Sponsor) is notified that PDREP-AIS has received the SAAR-P and is sent a link to review and approve/disapprove the SAAR-P.
- Approver (Supervisor/Sponsor) uses link provided from notification, reviews SAAR-P, then approves/disapproves SAAR-P.
 - If SAAR-P is disapproved, requester is notified of disapproval and SAAR-P is deleted from PDREP-AIS. Requester will need to submit another SAAR-P.
 - If SAAR-P is approved, requester is notified of approval and either a notification has been sent to the verifier or SAAR-P has been staged for PDREP-AIS Admin processing.
 - For NEW/RENEW SAAR-Ps, a notification has been sent to the Verifier (Security Manager) as listed on the SAAR-P.
 - For UPDATE SAAR-Ps without documented background investigation, a notification has been sent to the Verifier (Security Manager) as listed on the SAAR-P.
 - For UPDATE SAAR-Ps with documented background investigation, the SAAR-P will by-pass the Verifier and is staged for PDREP-AIS Admin audit/processing.
- Verifier (Security Manager) is notified that PDREP-AIS has received the SAAR-P and is sent a link to review and verify background investigation/reject the SAAR-P.
- Verifier (Security Manager) uses link provided from notification, reviews SAAR-P, then enters mandatory information and verifies/rejects SAAR-P.
 - If SAAR-P is rejected, requester is notified of rejection and SAAR-P is deleted from PDREP-AIS. Requester will need to submit another SAAR-P.
 - If SAAR-P is verified, requester is notified of verification SAAR-P has been staged for PDREP-AIS Admin processing.
- PDREP-AIS Admin performs audit of Submitted SAAR-P and requested accesses.
 - If special accesses are requested that need secondary approval (i.e. RIMS, SAM, ERS, QDR/SDR except Originator Point, etc.) or if additional information is required from Approvers or Verifiers, then POC notifications for special access/clarifications are sent to secondary approvers.

NOTE: *If requester selects access(es) that requires secondary approval(s), processing of the SAAR-P will be delayed until all secondary approvals are returned from POCs.*

- Secondary POC approvals/disapprovals sent to NSLC Help Desk for availability to PDREP-AIS Admins for processing.
- If SAAR-P does not pass PDREP-AIS Admin audit and is not processed, requester is notified and SAAR-P is deleted from PDREP-AIS. Requester will need to submit another SAAR-P.
- If SAAR-P passes PDREP-AIS Admin audit, SAAR-P is staged waiting for all secondary approvals.
- PDREP-AIS Admin processes SAAR-P and requester is notified of account processing and NEW requests are given a USER ID and instructions on how to obtain a temporary password.

3 ACCESSING THE SAAR-P

3.1 Users without Active Accounts

First time PDREP-AIS requesters/users with deactivated accounts will need to submit a SAAR-P (NEW/RENEW respectively), from the Product Data Reporting and Evaluation Program web page at <https://www.pdrep.csd.disa.mil> (See **Figure 3.1**).

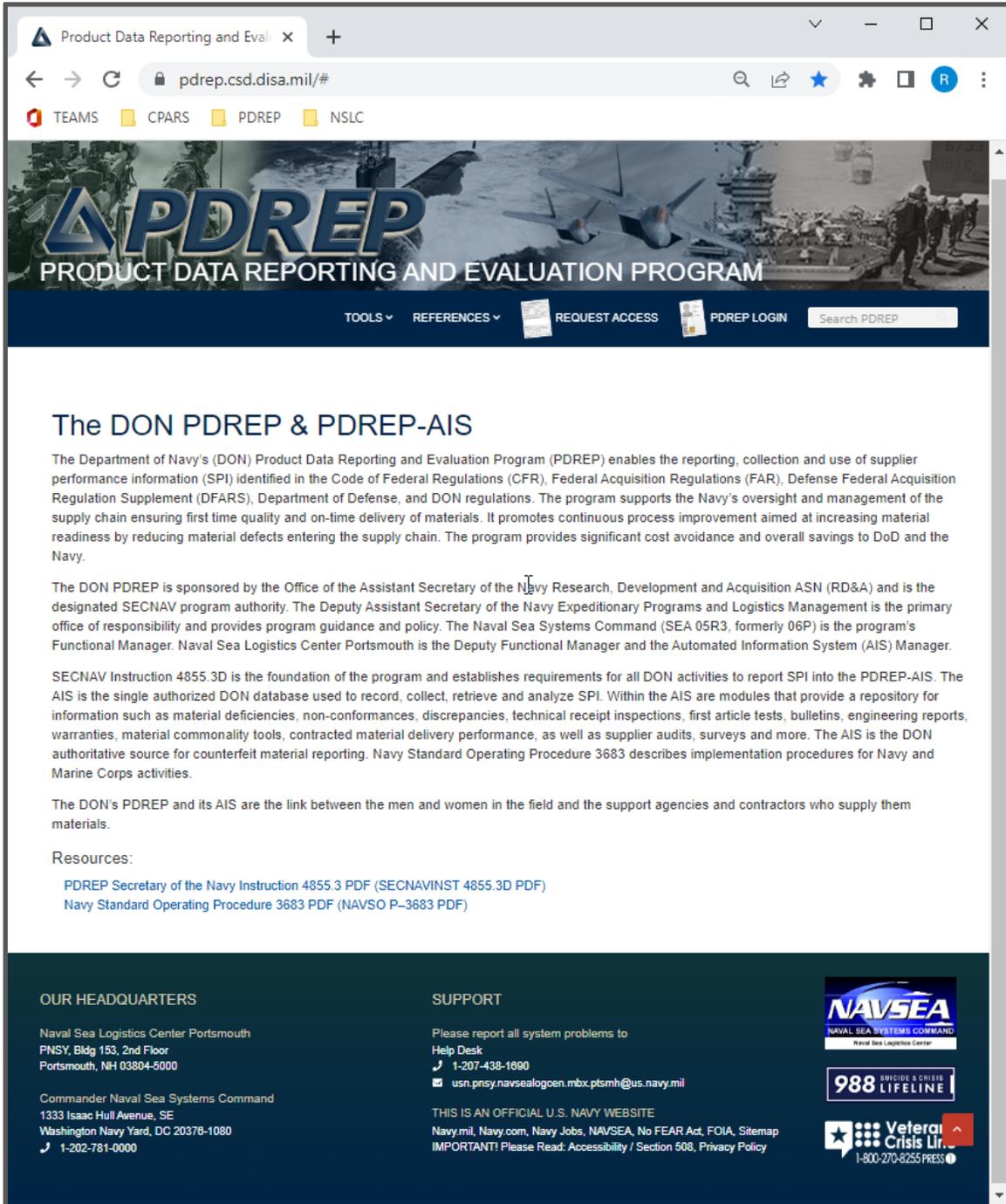


Figure 3.1

- Select 'REQUEST ACCESS' (See Figure 3.2)

The screenshot shows a web browser window with the URL pdrep.csd.disa.mil/#. The browser's address bar and tabs are visible at the top. Below the browser window is a navigation bar with the following items: TOOLS, REFERENCES, REQUEST ACCESS (highlighted with a blue arrow), PDREP LOGIN, and a search box labeled 'Search PDREP'. The main content area features a large banner with the PDREP logo and the text 'PRODUCT DATA REPORTING AND EVALUATION PROGRAM'. Below the banner is a section titled 'The DON PDREP & PDREP-AIS' with several paragraphs of text. At the bottom of the page, there are sections for 'OUR HEADQUARTERS', 'SUPPORT', and various logos including NAVSEA, 988, and the Veteran Crisis Line.

Product Data Reporting and Eval... x +

pdrep.csd.disa.mil/#

TEAMS CPARS PDREP NSLC

PDREP
PRODUCT DATA REPORTING AND EVALUATION PROGRAM

TOOLS REFERENCES REQUEST ACCESS PDREP LOGIN Search PDREP

The DON PDREP & PDREP-AIS

The Department of Navy's (DON) Product Data Reporting and Evaluation Program (PDREP) enables the reporting, collection and use of supplier performance information (SPI) identified in the Code of Federal Regulations (CFR), Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), Department of Defense, and DON regulations. The program supports the Navy's oversight and management of the supply chain ensuring first time quality and on-time delivery of materials. It promotes continuous process improvement aimed at increasing material readiness by reducing material defects entering the supply chain. The program provides significant cost avoidance and overall savings to DoD and the Navy.

The DON PDREP is sponsored by the Office of the Assistant Secretary of the Navy Research, Development and Acquisition ASN (RD&A) and is the designated SECNAV program authority. The Deputy Assistant Secretary of the Navy Expeditionary Programs and Logistics Management is the primary office of responsibility and provides program guidance and policy. The Naval Sea Systems Command (SEA 05R3, formerly 06P) is the program's Functional Manager. Naval Sea Logistics Center Portsmouth is the Deputy Functional Manager and the Automated Information System (AIS) Manager.

SECNAV Instruction 4855.3D is the foundation of the program and establishes requirements for all DON activities to report SPI into the PDREP-AIS. The AIS is the single authorized DON database used to record, collect, retrieve and analyze SPI. Within the AIS are modules that provide a repository for information such as material deficiencies, non-conformances, discrepancies, technical receipt inspections, first article tests, bulletins, engineering reports, warranties, material commonality tools, contracted material delivery performance, as well as supplier audits, surveys and more. The AIS is the DON authoritative source for counterfeit material reporting. Navy Standard Operating Procedure 3683 describes implementation procedures for Navy and Marine Corps activities.

The DON's PDREP and its AIS are the link between the men and women in the field and the support agencies and contractors who supply them materials.

Resources:

- [PDREP Secretary of the Navy Instruction 4855.3 PDF \(SECNAVINST 4855.3D PDF\)](#)
- [Navy Standard Operating Procedure 3683 PDF \(NAVSO P-3683 PDF\)](#)

OUR HEADQUARTERS

Naval Sea Logistics Center Portsmouth
PNSY, Bldg 153, 2nd Floor
Portsmouth, NH 03804-5000

Commander Naval Sea Systems Command
1333 Isaac Hull Avenue, SE
Washington Navy Yard, DC 20376-1080
1-202-781-0000

SUPPORT

Please report all system problems to
Help Desk
1-207-438-1690
usn.pnsy.navsealogoen.mbx.ptsmh@us.navy.mil

THIS IS AN OFFICIAL U.S. NAVY WEBSITE
Navy.mil, Navy.com, Navy Jobs, NAVSEA, No FEAR Act, FOIA, Sitemap
IMPORTANT! Please Read: Accessibility / Section 508, Privacy Policy

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Naval Sea Logistics Center

988
SUICIDE & CRISIS
LIFELINE

Veteran
Crisis Line
1-800-270-8255 PRESS 8

Figure 3.2

- Browser will navigate to the 'PDREP Account Type Definitions' page (See **Figure 3.3**).

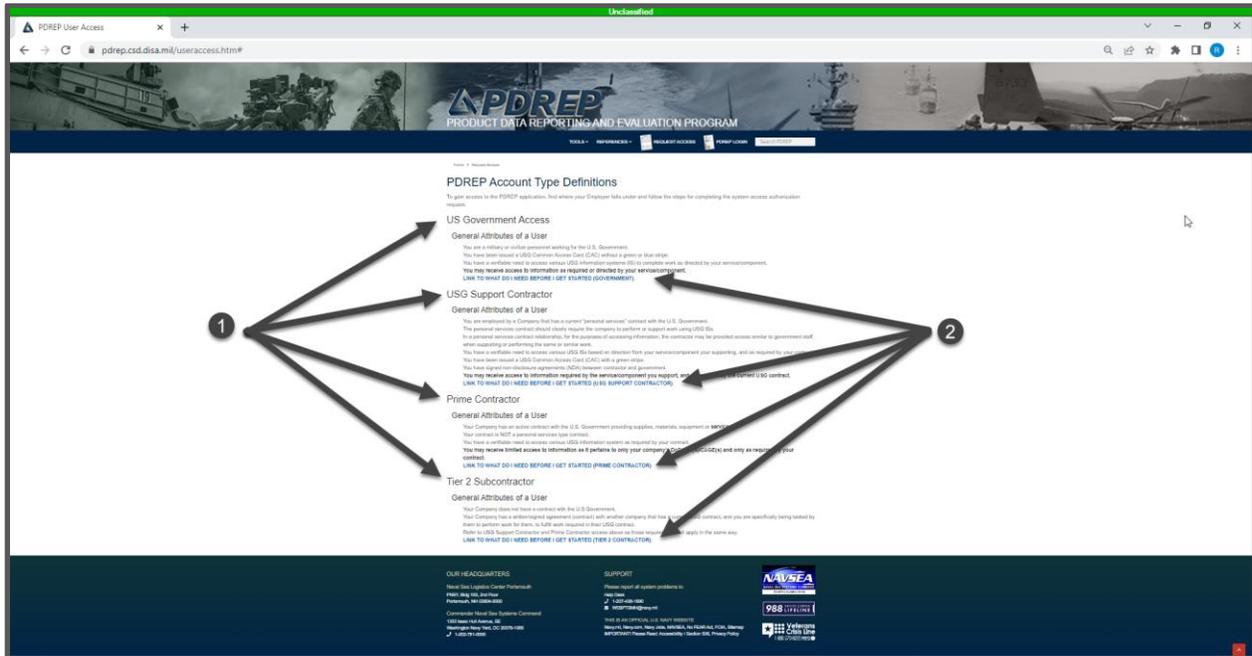


Figure 3.3

- Review the four types of accounts as outlined in Section 1 (See **Figure 3.3**, Item 1).
- Select 'WHAT DO I NEED TO GET STARTED' under the desired type of account (See **Figure 3.3**, Item 2).
- Browser will navigate to the 'What do I need before I Get Started' page (See example list for Tier 2 in **Figure 3.4**).

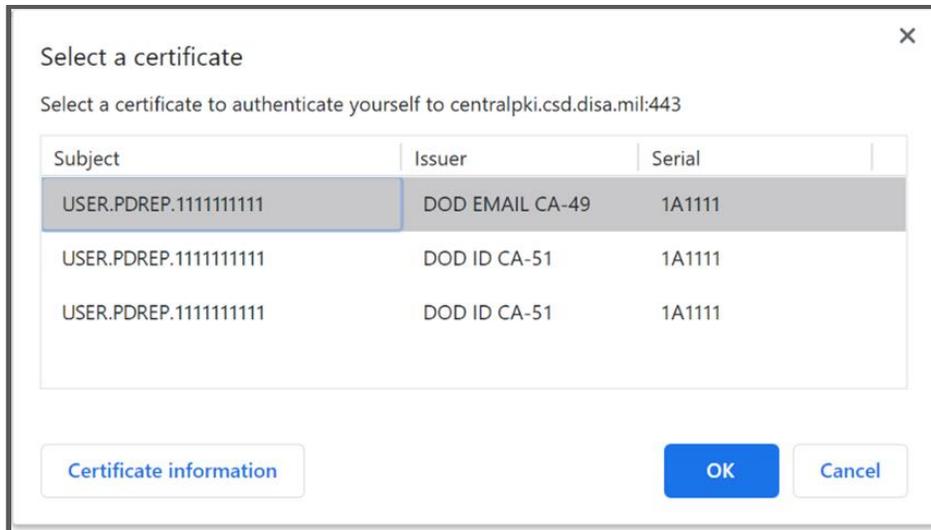


Figure 3.5a

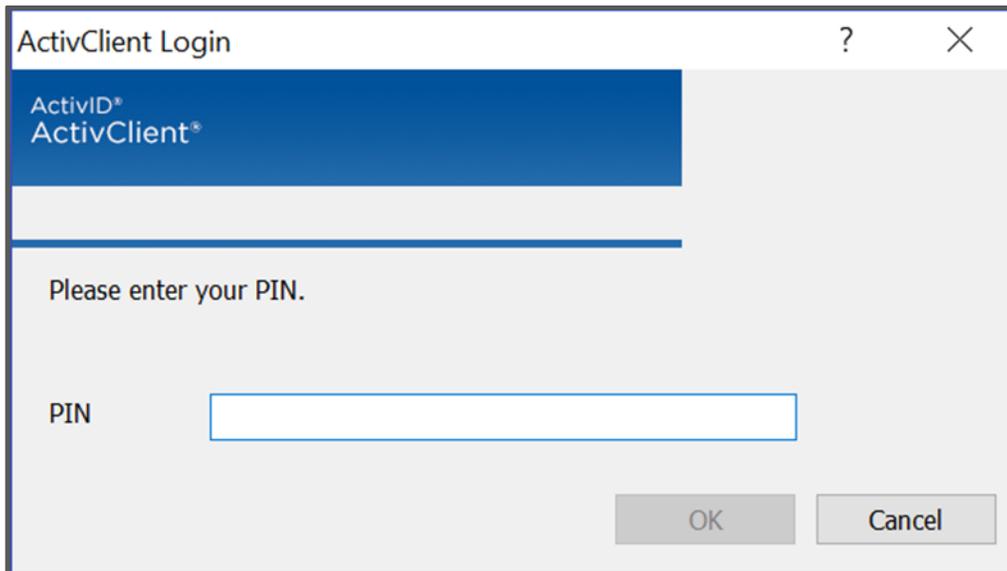


Figure 3.5b

- Browser will navigate to the DOD WARNING AND CONSENT BANNER (See Figure 3.6).



DOD WARNING AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Select Accept or Decline to continue.

 Accept Decline

Figure 3.6

- Select Accept. Selecting Decline will stop the process and return user to previous screen.
- Browser will navigate to SAAR-P with the "USER ACCESS REQUEST TYPE" (NEW) and user type prepopulated in the "I AM A" field (See **Figure 3.7**).

SYSTEM AUTHORIZATION ACCESS REQUEST - PDREP (SAAR-P)

Instructions
 (M) denotes a mandatory field
 1. Make sure the correct values for User Access Request Type and I AM A are selected
 2. Complete all Mandatory fields
 3. If known, select the PDREP Tool(s) you need
 4. The Comments section must explain why you need to use PDREP
 5. Select Read User Agreement and read it
 6. If you select I have read the agreement and agree to follow, you may then select Submit Request

USER ACCESS REQUEST TYPE: **I AM A:** 

User Information

(M) Last Name:

(M) First Name: Middle Initial:

(M) Primary DODAAC:

Secondary DODAAC:

DOD Activity Name:

Office Address:

City: State: Zip Code:

Office Symbol/Department:

(M) Area Code: (M) Work Phone Number: — Extension:

DSN: Fax:

Figure 3.7

3.2 Users with Active Accounts

Current users that need to update accesses will need to submit an UPDATE SAAR-P also referred to as an Access Change Request (See **Section 10.5**).

3.3 BETA Users without Active Accounts

First time BETA requesters/users with deactivated accounts will need to submit a SAAR-P (NEW/RENEW respectively), from the Product Data Reporting and Evaluation Program web page at <https://www.beta.pdrep.csd.disa.mil> (See **Figure 3.8**).

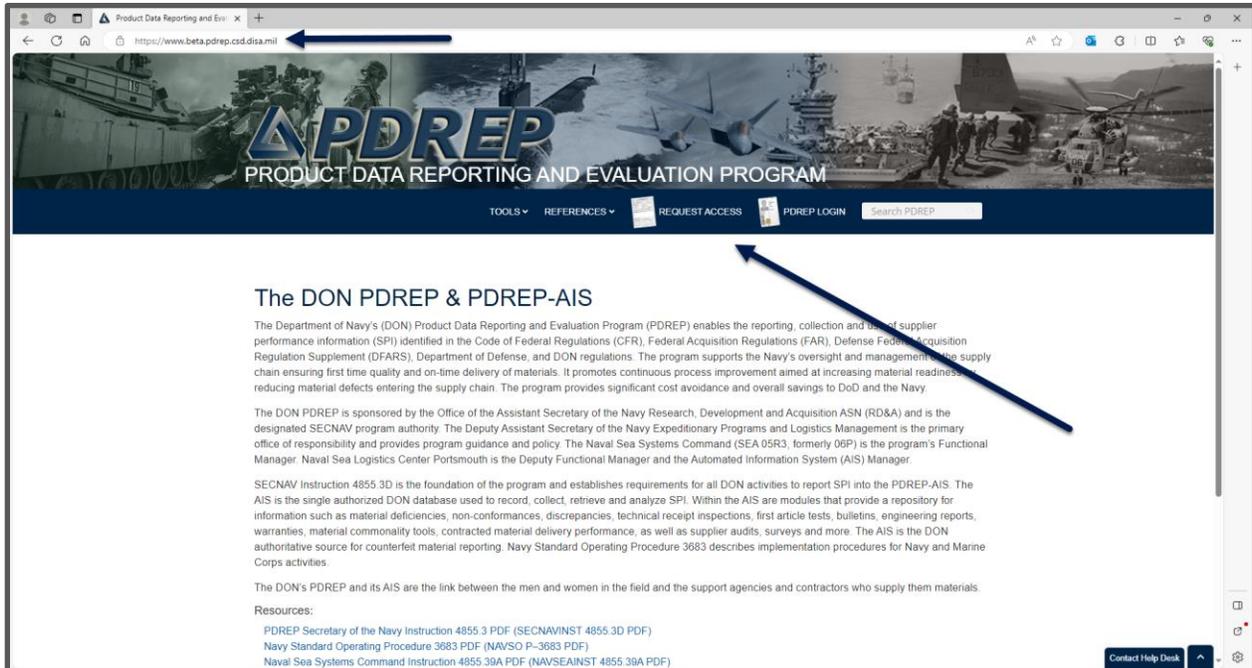


Figure 3.8

3.4 BETA Users with Active Accounts

Current BETA users that need to update accesses will need to submit an UPDATE SAAR-P also referred to as an Access Change Request (See **Section 10.5**) from within their BETA account.

4 COMPLETING THE SAAR-P (SUBMITTER)

4.1 Review Request Type

Verify the 'TYPE OF REQUEST' and adjust as required (See **Figure 4.1**, Item 1).

- NEW – If you select NEW and you have a deactivated PDREP account, you may get a new User ID and a new account and lose access to records in your current account.
 - Requester has never had a PDREP-AIS account.
 - Requester is reapplying but is switching between the four different account types (USG to CTR or CTR to USG).
 - Requester is reapplying but is changing component (i.e. USN to USA).

- RENEW
 - User account was deactivated because they did not login in the past 45 days.
 - User account was deactivated because contract had expired and replacement or extended contract is now in place.

- UPDATE
 - User has a current ACTIVE account.

NOTE: If User selects NEW and has a deactivated PDREP account, they may get a new User ID and a new account and lose access to records, stored ad-hocs, and work lists associated with deactivated account.

Verify 'I AM A' (account type) and adjust as required (See **Figure 4.1**, Item 2).

SYSTEM AUTHORIZATION ACCESS REQUEST - PDREP (SAAR-P)

Instructions
(M) denotes a mandatory field

1. Make sure the correct values for User Access Request Type and I AM A are selected
2. Complete all Mandatory fields
3. If known, select the PDREP Tool(s) you need
4. The Comments section must explain why you need to use PDREP
5. Select Read User Agreement and read it
6. If you select I have read the agreement and agree to follow, you may then select Submit Request

USER ACCESS REQUEST TYPE: NEW I AM A: Tier Two Ctr (SubCtr no current U.S.G contract)

Figure 4.1

4.2 User Information

Enter the following information:

- Last Name (Mandatory) (See **Figure 4.2**, Item 1).
- First Name (Mandatory) and Middle Initial (Optional) (See **Figure 4.2**, Item 2).

The screenshot shows a form titled "User Information" with the following fields and callouts:

- 1** (M) Last Name: [Text Input Field]
- 2** (M) First Name: [Text Input Field] Middle Initial: [Text Input Field]
- 3** (M) Primary DODAAC: [Text Input Field]
- Secondary DODAAC: [Text Input Field] Add Secondary DODAAC [Button]
- DOD Activity Name: [Text Input Field]
- Office Address: [Text Input Field]
- City: [Text Input Field] State: [Text Input Field] Zip Code: [Text Input Field]
- Office Symbol/Department: [Text Input Field]
- (M) Area Code: [Text Input Field] (M) Work Phone Number: [Text Input Field] - [Text Input Field] Extension: [Text Input Field]
- DSN: [Text Input Field] Fax: [Text Input Field]
- International Phone Number [Text Input Field]

Figure 4.2

- Primary DoDAAC (Mandatory) also known as “Activity” – Enter the Department of Defense Activity Address Code for the organization for which you primarily work (See Figure 5.2, Item 3). This auto fills the following information from PDREP-AIS data base:
 - DOD Activity Name (See **Figure 4.3**, Item 1).
 - Office Address (See **Figure 4.3**, Item 2).
 - City (See **Figure 4.3**, Item 3).
 - State (See **Figure 4.3**, Item 4).
 - Zip Code (See **Figure 4.3**, Item 5).

Note: *If this information is incorrect, user needs to contact Department of Defense Activity Address Directory (DoDAAD), the system of record for DoDAACs, not PDREP-AIS, to have this information updated. PDREP-AIS updates the DoDAAC tables from system of record on a regular basis.*

NOTE: *If a DCMA DoDAAC is entered, the ‘User Information’ block of the SAAR-P will update to include additional fields (See **Figure 4.4** and **Figure 4.5**).*

User Information

(M) Last Name:

(M) First Name: Middle Initial:

(M) Primary DODAAC:

1 Secondary DODAAC:

DOD Activity Name: MY WORK PLACE

2 Office Address: 123 MAIN STREET

3 City: ANYTOWN State: ST Zip Code: 12345-6789

4 Office Symbol/Department:

5

(M) Area Code: (M) Work Phone Number: - Extension:

DSN: Fax:

Figure 4.3

- Secondary DoDAAC (Optional) – If you perform work for multiple organizations, you may enter more than one DoDAAC.

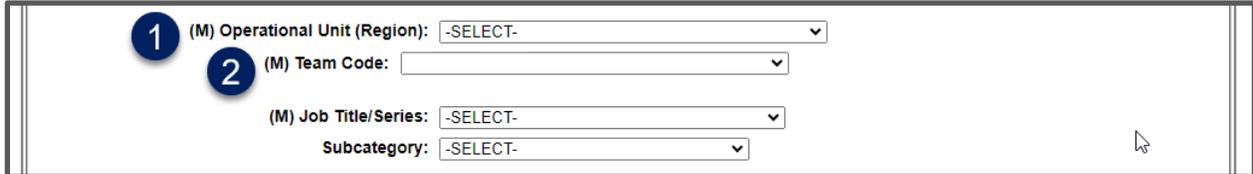
NOTE: Requesters will need to justify Secondary DoDAACs that are not within the same component (i.e. NAVSUP and NAVSEA or DLA and Army) as Primary DoDAAC.

- To add a Secondary DoDAAC to the SAAR-P:
 - Enter DoDAAC in Secondary DoDAAC field.
 - Select “Add Secondary DODAAC” button.
 - Secondary DoDAAC is added to Secondary DODAAC(s) table.
 - Repeat as required.
- To remove a Secondary DoDAAC from the SAAR-P:
 - Select DoDAAC in Secondary DoDAAC(s) table.
 - Select “Remove DODAAC” button.
 - Secondary DoDAAC is removed from Secondary DODAAC(s) table.
 - Repeat as required.
- Office Symbol/Department (Optional) for Non-DCMA. This becomes Team Code (Mandatory) for DCMA when a DCMA DoDAAC is entered in the Primary DoDAAC field.
- Commercial Phone Number:
 - Area Code (Mandatory).
 - Work Phone Number (Mandatory).
 - Extension (Optional).
- DSN (Optional).
- Fax (Optional).
- International Phone Number – This button will concatenate the commercial phone number and remove North America phone validation.

4.3 User information – Additional DCMA Fields

When a DCMA DoDAAC is entered as a Primary DoDAAC, the SAAR-P update to add the following fields. Select the following information from the Drop Down Lists (DDLs)

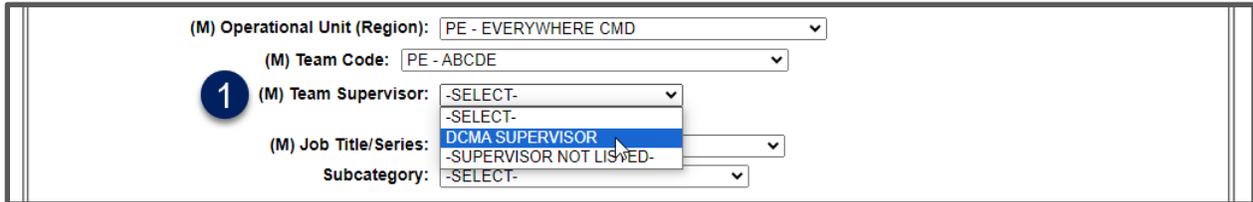
- Organizational Unit (Region) (Mandatory) – Select a unit from the drop down list. This will pre-populate the corresponding list in the Team Code drop down list (See **Figure 4.4**, Item 1).
- Team Code (Mandatory) – Select your team code from the drop down list. This will update the SAAR-P and add a supervisor field (See **Figure 4.4**, Item 2).



The screenshot shows a form with four mandatory dropdown menus. The first menu is labeled '(M) Operational Unit (Region):' with a value of '-SELECT-'. The second menu is labeled '(M) Team Code:' with a value of '-SELECT-'. The third menu is labeled '(M) Job Title/Series:' with a value of '-SELECT-'. The fourth menu is labeled 'Subcategory:' with a value of '-SELECT-'. A blue circle with the number '1' is next to the first menu, and a blue circle with the number '2' is next to the second menu.

Figure 4.4

- Team Supervisor (Mandatory) – Select the team supervisor from the drop down list. This will pre-populate supervisors email in the DoD Data Required block (See **Figure 4.5**, Item 1).



The screenshot shows the same form as Figure 4.4, but with the '(M) Team Supervisor:' dropdown menu open. The menu is highlighted with a blue circle and the number '1'. The menu options are: '-SELECT-', '-SELECT-', 'DCMA SUPERVISOR', '-SUPERVISOR NOT LISTED-', and '-SELECT-'. The other fields are filled with values: '(M) Operational Unit (Region):' is 'PE - EVERYWHERE CMD', '(M) Team Code:' is 'PE - ABCDE', '(M) Job Title/Series:' is '-SELECT-', and 'Subcategory:' is '-SELECT-'.

Figure 4.5

NOTE: *If you are the team supervisor, select your own name.*

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 on a monthly basis. If your supervisor is not listed or needs to be added for multiple teams, please have Supervisor update their profile in DCPDS to get added to the monthly list and have supervisor contact NSLC Portsmouth Help Desk to request to be temporarily added to the DDL.*

- Job Title/Series (Mandatory) - Select applicable item from drop down list (See **Figure 4.6**).

(M) Job Title/Series:

Subcategory:

(M) Area Code: (M) Work

DSN:

International Phone

Extension:

- AIRCRAFT OPERATIONS
- BUDGET ANALYST
- COMPUTER ENGR
- CONTRACT SPEC
- GENERAL ENGR
- GOVERNMENT FLIGHT REP
- INDUSTRIAL PROPERTY
- INDUSTRIAL SPEC, GEN
- INTERDISC ENGR, AEROSPACE
- INTERDISC ENGR, ELECTRONICS
- INTERDISC ENGR, INDUSTRIAL
- INTERDISC ENGR, MECH
- IT SPEC, DATAMGT
- LOGISTICS MGMT SPEC
- MANAGEMENT AND PROGRAM ANALYST
- MAT ENGR
- OPERATIONS RESEARCH ANALYST
- PACKAGING SPEC
- PM
- QA SPEC
- SAFETY, OCCUP HEALTH MGR
- TRAFFIC MGMT SPEC
- TRANSPORTATION ASST

Figure 4.6

- Subcategory (Conditionally Mandatory for Contract Spec only) - Select applicable item from drop down list (See **Figure 4.7**).

(M) Operational Unit (Region):

(M) Team Code:

(M) Team Supervisor:

(M) Job Title/Series:

Subcategory:

(M) Area Code: (M) Work

DSN:

International Phone Number

Extension:

- SELECT-
- CONTRACT SPEC
- CONTRACT SPEC, PROCURE ANLYT
- PROCUREMENT ANLYT
- CONTRACT ADMIN, ACO

Figure 4.7

4.4 DoD Contractor Data Required (Contractors Only)

Enter the following information:

- Contract Number (Mandatory) – This is the instrument that identifies your need to access/work in a government data base. DOD Contracts starting FY 17 use Procurement Instrument Identifier (PIID) format (13 characters) (See **Figure 4.8**, Item 1):
 - Office issuing instrument (typically DoDAAC) (6 alpha numeric).
 - Last 2 digits of Fiscal Year PIID was issued (2 numeric).
 - Instrument Type (1 alpha).
 - Assigned serial number (4 alpha numeric).

NOTE: *If contract numbers cannot be verified in FPDS-NG or PDREP-AIS CAD module, SAAR-P may be rejected at PDREP-AIS Admin audit stage.*

- Contract End Date (Mandatory) (See **Figure 4.8**, Item 2).
- CAGE (Commercial and Government Entity) (Mandatory) – This identifies the company on the contract. After entering the CAGE, the following information will be displayed (See **Figure 4.8**, Item 3):
 - Company Name.
 - Company Address.
 - City.
 - State.
 - Zip Code.

Note: *If this information is incorrect, user needs to contact SAM.GOV, the system of record for CAGE Codes, not PDREP-AIS, to have this information updated. PDREP-AIS updates the CAGE Code tables from system of record on a regular basis. Also note to which company the CAGE Code identifies:*

- Support Contractor – This is your company. This is not the location of the government entity where you are working.
 - Prime Contractor – This is your company. This is not the location of the government entity where you are working if working on-site.
 - Tier 2 Subcontractor – This is not your company. This is the company (Tier 1) that is on the contract that subcontracted work to your company.
- Sponsor Phone Number (See **Figure 4.8**, Item 4).
 - Area code (Mandatory).
 - Sponsor Work Phone Number (Mandatory).
 - Extension (Optional).

- Fax (Optional) (See **Figure 4.8**, Item 5).
- International Phone Number – This button will concatenate the commercial phone number and remove North America phone validation (See **Figure 4.8**, Item 6).

DoD Contractor Data Required

(M) Contract Number: (M) Contract End Date:

(M) CAGE:

Company Name:

Company Address:

City:

State: Zip Code:

(M) Sponsor Area Code: (M) Sponsor Work Phone Number: - Extension:

Fax:

Figure 4.8

4.5 DoD Data Required

Enter the following information:

- Submitter Email Address (Mandatory) – Submitter’s official e-mail address (i.e. first.last@mail.mil) USG and Support Contractors extensions should be .mil but can be ‘.org’ or ‘.gov’ but not ‘.com’. Requesters should use their individual official e-mail not a group e-mail account. Personal e-mail is not authorized (gmail, hotmail, yahoo, etc.) (See **Figure 4.9**, Item 1).
- Sponsor/Supervisor Email Address (Mandatory) – Submitter’s supervisor (or their representative) e-mail address. May not be a contractor (See **Figure 4.9**, Item 2).
 - Not requester’s email as a supervisor.
 - Cannot be same as requester’s e-mail address. You cannot be your own supervisor.
 - For DCMA, this is prepopulated by selecting Supervisor from drop down list.

NOTE: *For DCMA, if you are the team supervisor and your e-mail appears here, manually insert your actual supervisors e-mail address in place of your own e-mail address.*

NOTE: *Sponsor should be (but not required to be) a contracting officer. They need to be able to verify submitter/company relationship, contract validity, contract end date, users need for access, type access allowed by contract, modules required and subcontract (if Tier 2 requester).*

NOTE: *Sponsor needs to be a US Government employee (Civilian or military) and not a contractor.*

NOTE: *Ensure the Supervisor/Sponsor’s e-mail address is correct. Your Supervisor/Sponsor will receive a notification about your access request and is required to subsequently approve the need for access to the PDREP-AIS. This cannot be changed, only deleted, and submitter will have to resubmit SAAR-P if e-mail address is invalid.*

- Security Manager’s e-mail address (Optional at Submitter stage) (See **Figure 4.9**, Item 3).

NOTE: *Ensure the Security Manager’s e-mail address is correct, if entered. The Security Manager will receive a notification about submitter access request and is required to subsequently verify submitter background investigation for access to the PDREP-AIS. This can be changed by Supervisor/Sponsor prior to approval. This cannot be changed by PDREP-AIS Admins. SAAR-Ps can only be deleted from the queue, and submitter will have to resubmit another SAAR-P if e-mail address is invalid.*

NOTE: *If submitter enters either the submitters email or supervisor e-mail for Security Manager e-mail, SAAR-P will be delayed until Security Manager returns a digitally signed e-mail to NSLC Portsmouth Help Desk stating that they occupy both positions.*

DoD Data Required	
(M) Submitter Email Address:	<input type="text"/>
(M) Sponsor/Supervisor Email Address:	<input type="text"/>
Security Manager Email Address:	<input type="text"/>



Figure 4.9

4.6 Request Access Levels

SAAR-P access level availability will vary, depending on type of account (USG or CTR) and components (ARMY, DCMA, etc.) 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'.

Unless otherwise noted, default access is non-management. If management access is required, put notation in justification field.

NOTE: *Only select access that pertains to your duty and/or Agency and/or need. While submitters may request for access to any module, they 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 contains Controlled Unclassified Information (CUI), so selections should be made for lawful government need for access. Refer to individual module user guides for applicability for each module.*

Select accesses as required (See **Figure 4.12**):

- Product Quality Deficiency Report - PQDR Application: Select the boxes for the access levels required.
 - View Only – Allows viewing of PQDR data. Selecting this will deselect and lock out all other accesses. If you need one of the other accesses, deselect View Only.
 - Originating Point – Receives/reports deficient material and submits PQDR.
 - Screening Point – A focal point for component PQDRs, validates accuracy of data, and forwards to Action Point for investigation.
 - Action Point – Responsible for investigation into root cause of deficiency. May delegate investigation to Support Point.
 - Support Point – Performs investigation into root cause of deficiency at request of Action Point.
- PQDR Army only – When an Army DoDAAC is entered as a Primary DoDAAC, a drop down list containing “-SELECT-, Master Screener, Action Officer, and Both” will appear (See **Figure 4.10**).
 - Selecting Master Screener from the list will select and lock Screening Point check box (and give Management Access) but will allow selection of other check boxes. To deselect Screening Point check box, you need to select one of the other options in the drop down list or select View Only.
 - Selecting Action Officer from the list will select and lock Action Point check box (and give Management Access) but will allow selection of other check

boxes. To deselect Action Point check box, you need to select one of the other options in the drop down list or select View Only.

- Selecting Both from the list will select and lock Screening Point and Action Point check boxes (and give Management Access) but will allow selection of other check boxes. To deselect either Screening Point or Action Point check boxes, you need to select one of the other options in the drop down list or select View Only.

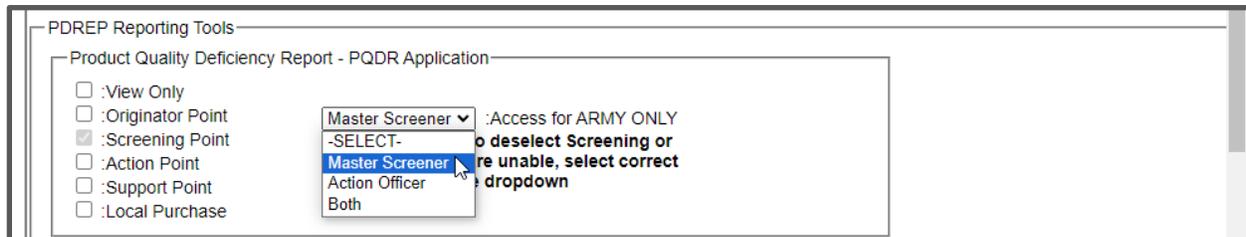


Figure 4.10

- PQDR DCMA only – When an DCMA DoDAAC is entered as a Primary DoDAAC, a drop down list containing “-SELECT-, QAR, and DRPM” will appear (See **Figure 4.11**).
 - Selecting QAR from the list will select and lock Originator Point and Support Point check boxes (and give Non-Management Access) but will allow selection of other check boxes. To deselect either Originator Point and Support Point check boxes, you need to select -SELECT- in the drop down list or select View Only.
 - Selecting DRPM from the list will select and lock Originator Point and Support Point check boxes (and give Management Access) but will allow selection of other check boxes. To deselect either Originator Point and Support Point check boxes, you need to select -SELECT- in the drop down list or select View Only.

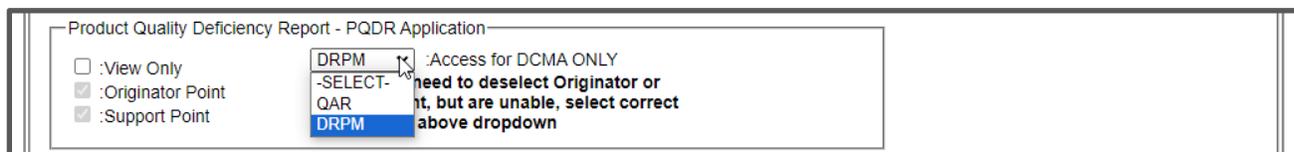


Figure 4.11

- Supply Discrepancy Reports – SDR Application: Select the boxes for the access levels required.
 - View Only – Allows viewing of SDR data. Selecting this will lock out all other accesses. If you need one of the other accesses, deselect View Only.

- Originator Point – Receives/Reports discrepant material and submits SDR.
- Action Point – Investigates/reports cause of discrepancy and determines disposition.
- RIMS/SAM/ERS NNPI – Only select Nuclear User check box if you are authorized access to any of these modules and you work in the nuclear environment.
- Receipt Inspection Management System (RIMS). Typically pertains to Naval Shipyards and Navy Warfare Centers.
 - Select your user role form the RIMS drop down list.
 - Select CIM user only if Controlled Industrial Material pertains to you.
- Supply Action Module (SAM) - Select your user role form the SAM drop down list.
- Corrective Action Request (CAR) - Select your user role form the drop down list.
- Quality Assurance Letter of Instruction (QALIs) and Letters of Delegation (LODs) – Select your user role form the drop down list.
- Surveillance Plan (SP) - Select your user role form the drop down list.
- Engineering Referral System - ERS Application: Select the boxes for the access levels required. Selecting the Management check box will yield management level access for all levels selected.
- SPPI Bulletins (SB) - Select your access level form the drop down list.
- Supplier Risk System (SRS) - Select your access level form the drop down list.
- Other PDREP Tools: Check the boxes that apply to your requirements.
 - NAVSUP Level I/SUBSAFE Stock Search.
 - Material Inspection Record (MIR).
 - Contract Award and Delivery Data (CAD).
 - Test Records (TST).
 - Survey Records (SRV).
 - Special Quality Data (SQD).
 - Supplier Audits & Assessments (SAA).
 - Receive SPPI Bulletins (SB).
 - Supplier Audits & Assessments Alerts.
 - Contractor Profile.
 - Material Profile.
 - Warranty.
 - NAVSUP Level 1 Report.

PDREP Reporting Tools

Product Quality Deficiency Report - PQDR Application

- :View Only
- :Originator Point
- :Screening Point
- :Action Point
- :Support Point
- :Local Purchase

Supply Discrepancy Report - SDR Application

- :View Only
- :Originator Point
- :Action Point

RIMS/SAM/ERS NNPI

- :Nuclear User

Receipt Inspection Management System (RIMS)

:Receipt Inspection Management System (RIMS)

- :CIM User

Supply Action Module (SAM)

:Supply Action Module (SAM)

Corrective Action Request(CAR)

User Role:

Quality Assurance Letter of Instruction (QALIs) and Letters of Delegation (LODs)

User Role:

Surveillance Plan (SP)

User Role:

Engineering Referral System - ERS Application

- :Originator Point
- :Screening Point
- :Action Point
- :Management

SPPI Bulletins (SB)

:Create/Edit/Search SPPI Bulletins (SB)

Supplier Risk System (SRS)

:Supplier Risk System (SRS)

Other PDREP Tools

- :NAVSUP Level I/SUBSAFE Stock Search
- :Material Inspection Record (MIR)
- :Contract Award and Delivery Data (CAD)
- :Test Records (TST)
- :Survey Records (SRV)
- :Special Quality Data (SQD)
- :Supplier Audits & Assessments (SAA)
- :Receive SPPI Bulletins (SB)
- :Supplier Audits & Assessments Alerts
- :Contractor Profile
- :Material Profile
- :Warranty
- :NAVSUP Level 1 Report

Figure 4.12

4.7 Citizenship and Training Confirmations (Mandatory) (See Figure 4.13).

- Select U.S. Citizen, Foreign National, or Other as applicable.
- Select the Annual Cyber Awareness Training check box if applicable. If Submitter has not completed their annual cyber training, then SAAR-P cannot be submitted.
- Enter Date of Annual Cyber Awareness Training by either selecting date using calendar button, or entering date using MM/DD/YYYY format.
- Select additional check U-NNPI training check box. This will only appear if submitter selected the NNPI check box in the select accesses section above.

(M) Citizenship and Training Confirmations

I hereby confirm that I am a:

U.S. Citizen Foreign National Other

I have completed the Annual Cyber Awareness Training. Date:

I have completed my required U-NNPI Training.

Figure 4.13

NOTE: *The ANNUAL CYBER AWARENESS TRAINING is not a PDREP sponsored class. This is your components requirement.*

4.8 Justification for Access (Mandatory) (See Figure 4.14)

Enter pertinent information for approvers as to why PDREP-AIS access is required and any notes for PDREP Admins as to why access variations are needed as described in above Notes.

(M) Justification for Access

Figure 4.14

NOTE: *The Justification for Access notes are included in the notifications to the Supervisor/Sponsor and Security Manager.*

4.9 Read and Agree to User Agreement

- Select 'to read the agreement' (Mandatory) (See **Figure 4.15**).

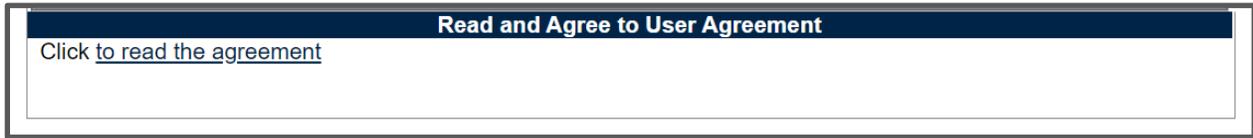


Figure 4.15

- The user agreement appears in a pop-up window.
- Read and scroll through user agreement.
- At the end of the user agreement (See **Figure 4.16**), select either:
 - 'I have read the agreement and agree to follow' which will navigate browser back to SAAR-P with a sign and submit button.
 - 'I do not agree' which will navigate browser back to SAAR-P.

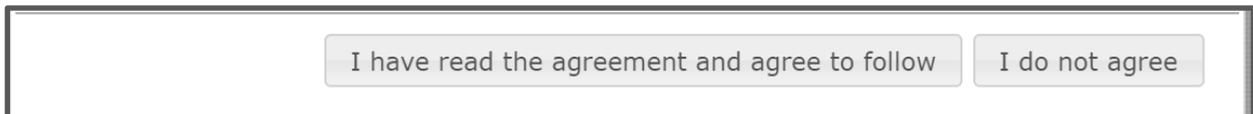


Figure 4.16

4.10 Sign and Submit SAAR-P

- Select the 'Sign and Submit Request' button (See **Figure 4.17**).



Figure 4.17

NOTE: *Submitter is DIGITALLY SIGNING affirmation to the User Agreement and that all information on SAAR-P is correct. SAAR-P is stamped with user information from CAC/Cert.*

- After selecting the 'Sign and Submit Request' button, user will receive a confirmation (See **Figure 4.18**). The PDREP ID is not your User ID. This is the SAAR-P serial number for tracking purposes. If you do not see this confirmation, your SAAR-P was not submitted successfully.

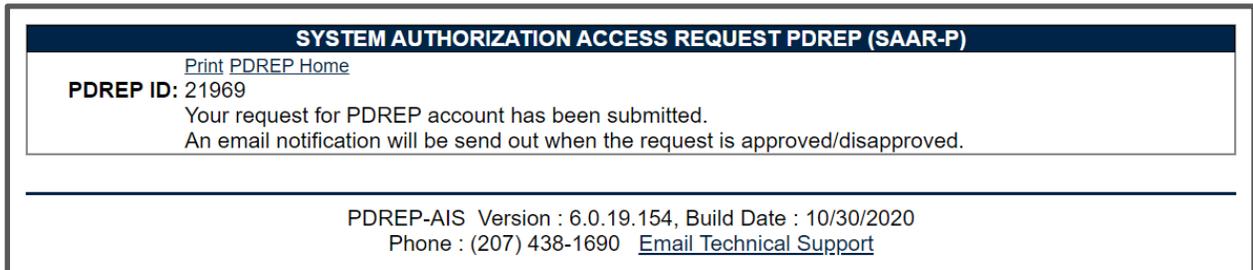


Figure 4.18

- 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. See **Appendix 1** – Notifications.

5 APPROVING THE SAAR-P (SUPERVISOR/SPONSOR)

5.1 Accessing SAAR-P

- Approver (Supervisor/Sponsor) receives e-mail identifying requester and includes a URL for navigation to approval page. See **Appendix 1** – Notifications.
- Approver selects URL or copies/pastes URL into browser. For security purposes, approvers' IT systems may add extraneous characters to the URL.

- Example for NAVY - Sent from PDREP:

`https://centralpki.csd.disa.mil/pki/checkcert?appname=pdrepgovttest&loginredirect=requestaccountsupervisor&requestaccountseq=ABCDEF123DEFGHI456GHIJKL789JKLMNO`

- Example - received by approver:

`<https://noclick.mil/?https://centralpki.csd.disa.mil/pki/checkcert?appname=pdrepgovttest&loginredirect=requestaccountsupervisor&requestaccountseq=ABCDEF123DEFGHI456GHIJKL789JKLMNO>`

- Approver may need to select certificate (See **Figure 5.1a**).
- Approver may need to enter CAC/PIV/Certificate PIN (See **Figure 5.1b**).

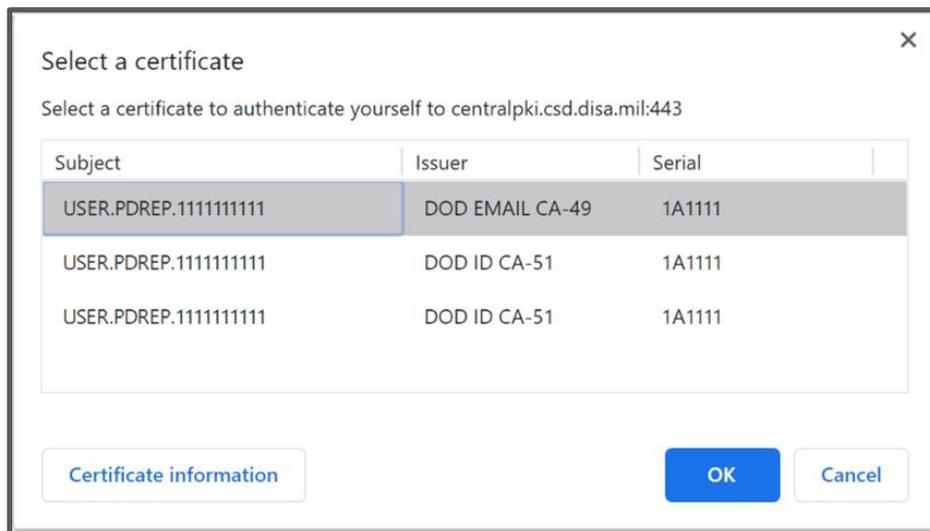


Figure 5.1a

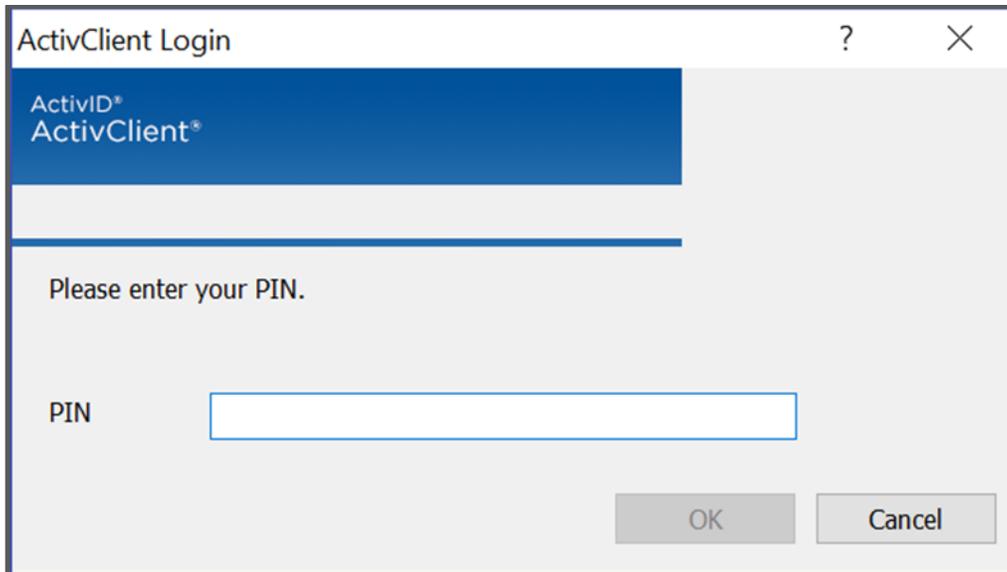


Figure 5.1b

- Browser is then navigated to the 'DOD WARNING AND CONSENT BANNER' page (See **Figure 5.2**).

PDREP
Product Data Reporting and Evaluation Program

DOD WARNING AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Select Accept or Decline to continue.

Accept Decline

Figure 5.2

- Select Accept. Selecting Decline will stop the process and return user to previous screen.
- Browser will navigate to display only version of SAAR-P with the “USER ACCESS REQUEST TYPE” (NEW/RENEW/UPDATE) and user type prepopulated in the “I AM A” field (See **Figure 5.3**).

5.2 Validating SAAR-P

- Approver Validates User Information (See **Figure 5.3**).
 - Type of request – New, Renew, or Update.
 - “I Am A” field (type of user) Ensure they are either a US Government Employee (mil/civ) or Contractor as selected.
 - User Information – Name, DoDAAC, phone, and e-mail.
 - US Government Employees (Civilian/Military) DoDAAC typically start with F, H, J, M, N, R, S, V, W, or Z or must provide justification for access to prime contractor records.
 - Support contractors DoDAAC typically start with F, H, J, M, N, R, S, V, W, or Z.
 - Prime Contractors DoDAAC must start with O, C, E, L, Q, or U.
 - Subcontractors DoDAAC follows Tier1 Company’s contract (Support or Prime listed above).
- Approver enters/updates “Security Managers Email Address” for background verification if not entered by submitter.

NOTE: *Ensure the Security Manager’s e-mail address is correct. The Security Manager will receive a notification about submitter access request and is required to subsequently verify submitter background investigation for access to the PDREP-AIS. This cannot be changed by PDREP-AIS Admins. SAAR-Ps can only be deleted from the queue, and submitter will have to resubmit another SAAR-P if e-mail address is invalid.*

SYSTEM AUTHORIZATION ACCESS REQUEST- PDREP (SAAR-P) - CERTIFIER APPROVAL

Instructions
 The USG supervisor, their representative, or the USG sponsor of non-USG personnel should review the request for accuracy and validate the need for access to the data contained in the PDREP-AIS Module as requested.

Do NOT approve requests in cases where:
 1. You do not know the person making the request for access to the PDREP-AIS.
 2. You are not the requestor's USG supervisor, their representative, the Information Owner, or the USG sponsor (i.e. contracting officer aware of the contract and the contractors valid need to access the USG Information system)
 3. Cannot validate the business related need for access to any of the data contained in the PDREP-AIS Module being requested.

User Access Request Type: **NEW** IAMA: U.S.G Employee

User Information

Last Name: EMPLOYEE		First Name: USG Middle Initial:	
Primary DODAAC: DODAAC			
List of Secondary DODAAC(s):			
DOD Activity Name: PRIMARY ACTIVITY			
Office Address: 123 MAIN ST			
City: ANYTOWN		State: ST	Zip Code: 12345 - 6789
Work Phone/Ext: 888-555-1212		DSN:	Fax:
Submitter Email Address: USG.EMPLOYEE.CIV@MAIL.MIL			
(M) Certifier Email Address: APPROVER.E-MAIL.CIV@MAIL.MIL			
(M) Security Manager Email Address: _____			

Figure 5.3

- Approver validates Contract information (Sponsors Only) (See **Figure 5.4**):

- Contract number is valid.
- Sponsor validates contract end date.
- CAGE/company on SAAR-P is CAGE/Company on Contract.
- Sponsor validates sponsor phone number.

Please verify the following information:

(M) Contract Number: DODAAC23D1234			(M) Contract End Date: 09/30/2023		
(M) CAGE: CAGE1					
Company Name: CO INC					
Company Address: 123 OAK ST					
City: CITY		State: ST		Zip Code: 12345-1234	
(M) Work Phone: 800-555-1212		Ext:		Fax:	

Figure 5.4

- Approver validates accesses requested (See **Figure 5.5**).

PDREP Reporting Tools

Product Quality Deficiency Report - PQDR Application

:Originator Point

Supply Discrepancy Report - SDR Application

:Originator Point

RIMS/SAM/ERS NNPI

Receipt Inspection Management System (RIMS)

:Receipt Inspection Management System (RIMS)

Supply Action Mode (SAM)

:Supply Action Mode (SAM)

Corrective Action Request (CAR)

User Role:

Quality Assurance Letter of Instruction (QALIs) and Letters of Delegation (LODs)

Surveillance Plan (SP)

User Role:

Engineering Referral System - ERS Application

SPPI Bulletins (SB)

:Create/Edit/Search SPPI Bulletins (SB)

Supplier Risk System (SRS)

:Supplier Risk System (SRS)

Other PDREP Tools

:Material Inspection Record (MIR)

:Contract Award and Delivery Data (CAD)

:Contractor Profile

Figure 5.5

- Approver validates Citizenship and Training (See **Figure 5.6**).



Citizenship and Training Confirmations
I hereby confirm that I am a: U.S. Citizen Foreign National Other
 I have completed the Annual Cyber Awareness Training. Date: 09/01/2023

Figure 5.6

- Approver validates Submitter Digital Signature and Date (See **Figure 5.7**).



Signatures
Submitter Date: 09/19/2023 Signature: CONTRACTOR_SUPPORT.0123456789
Approver Date: Signature:

Figure 5.7

- Approver enters comments that will be included in the notification to submitter. This is **OPTIONAL** for Approval but **MANDATORY** for Disapprovals (See **Figure 5.8**).



(CM) Approver Comments (will be appended to email sent to user)

Figure 5.8

5.3 Certifying User/Self Type and Contract Information

- Approver checks corresponding box certifying (See **Figures 5.9 through 5.12**). Only one of the below sets of check boxes will appear, depending on the type of user.
 - Type of user.
 - Approver is a USG Employee.
 - Approver is supervisor (or representative) for USG employees.
 - Validated the need for PRDEP access.
 - Validated contract information.

US Government Employee

By selecting this box, I certify the following:

I certify that the submitter is a US Government employee (Military/Civilian).
 I certify that I am a US Government employee (Military/Civilian).
 I certify that I am the submitter's supervisor or authorized to sign for the submitter's supervisor.
 I certify the submitter has a lawful government need for access to data/modules requested.

Figure 5.9

US Support Contractor

By selecting this box, I certify the following:

I certify that the submitter is not a US Government employee (Contractor).
 I certify that I am a US Government employee (Military/Civilian).
 I certify that I have reviewed the contract listed and company listed above is on the contract listed above.
 I certify the submitter is an employee of the company listed has a lawful government need for access (via contract) to data/modules requested.
 I certify the contract listed is a personal services type contract or there is specific verbiage/clauses as outlined in FAR 37.104 that allow the submitter to be treated as government employee.
 I certify there is a Non-Disclosure Agreement in place between the submitter/Company and the U.S Government.

Figure 5.10

Prime Contractor

By selecting this box, I certify the following:

I certify that the submitter is not a US Government employee (Contractor).
 I certify that I am a US Government employee (Military/Civilian).
 I certify that I have reviewed the contract listed and company listed above is on the contract listed above.
 I certify the submitter is an employee of the company listed has a lawful government need for access (via contract) to data/modules requested.

Figure 5.11

Tier 2 Subcontractor

By selecting this box, I certify the following:

- () I certify that the submitter is not a US Government employee (Contractor).
- () I certify that I am a US Government employee (Military/Civilian).
- () I certify that I have reviewed the contract listed and company listed above is on the contract listed above.
- () I certify the submitter is NOT an employee of the company listed on the contract above.
- () I certify I have reviewed the signed agreement between the Company listed on the contract (Tier 1) and the company that the submitter works (Tier 2) and that the submitter is an authorized agent of the Tier 1 contractor.
- () I certify the submitter has a lawful government need (via contract and sub-contract/agreement) for access to data/modules requested.
- () I certify the contract listed is a personal services type contract or there is specific verbiage/clauses as outlined in FAR 37.104 that allow the submitter to be treated as government employee if Tier 1 is a Support Contractor.

Figure 5.12

5.4 Approving or Disapproving SAAR-P

To approve request, select 'Approve and Sign'.

- Approver's browser will be navigated to a confirmation screen (See **Figure 5.13**).
- Requester is notified of Supervisor/Sponsor approval (See **Appendix 1 – Notifications**).
- Notifications are sent to POCs for accesses that require secondary approvals (See Appendix 1 – Notifications).

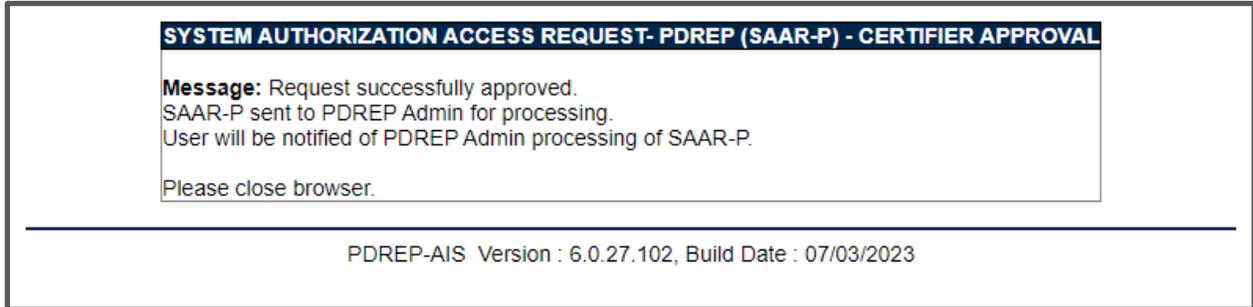


Figure 5.13

NOTE: When selecting "Approve and Sign", approver is *DIGITALLY SIGNING* that they have verified all the information as outlined above and the SAAR-P will be digitally signed and stamped with approver information from CAC/PIV.

To disapprove a SAAR-P, select "Disapprove"

- Approver's browser will be navigated to a confirmation screen (See **Figure 5.14**).
- Requester is notified of Supervisor/Sponsor disapproval (See **Appendix 1 – Notifications**).



Figure 5.14

6 VERIFYING SUBMITTER BACKGROUND (SECURITY MANAGER)

6.1 Accessing SAAR-P

- Verifier (Security Manager) receives e-mail identifying requester and includes a URL for navigation to approval page. See **Appendix 1** – Notifications.
- Verifier selects URL or copies/pastes URL into browser. For security purposes, verifiers' IT systems may add extraneous characters to the URL.

- Example for NAVY - Sent from PDREP:

`https://centralpki.csd.disa.mil/pki/checkcert?appname=pdrepgovttest&loginredirect=requestaccountsupervisor&requestaccountseq=ABCDEFGHI456GHIJKL789JKLMNO`

- Example - received by verifier:

`<https://noclick.mil/?https://centralpki.csd.disa.mil/pki/checkcert?appname=pdrepgovttest&loginredirect=requestaccountsupervisor&requestaccountseq=ABCDEFGHI456GHIJKL789JKLMNO>`

- Verifier may need to select certificate (See **Figure 6.1a**).
- Verifier may need to enter CAC/PIV/Certificate PIN (See **Figure 6.1b**).

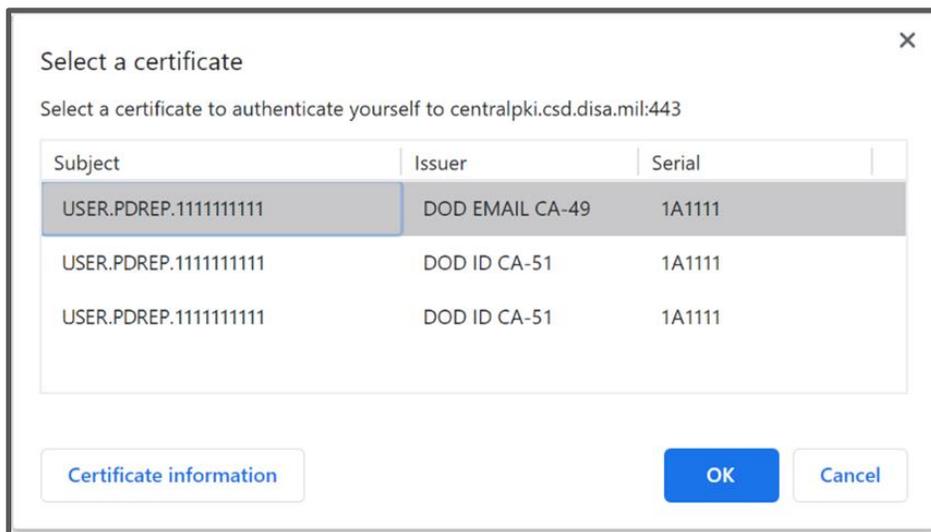


Figure 6.1a

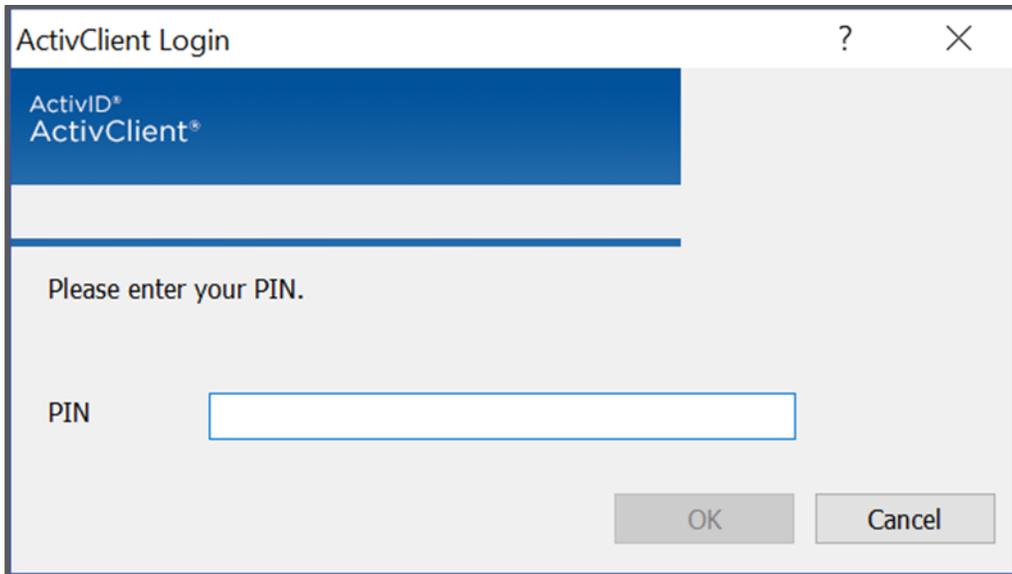


Figure 6.1b

- Browser is then navigated to the 'DOD WARNING AND CONSENT BANNER' page (See **Figure 6.2**).

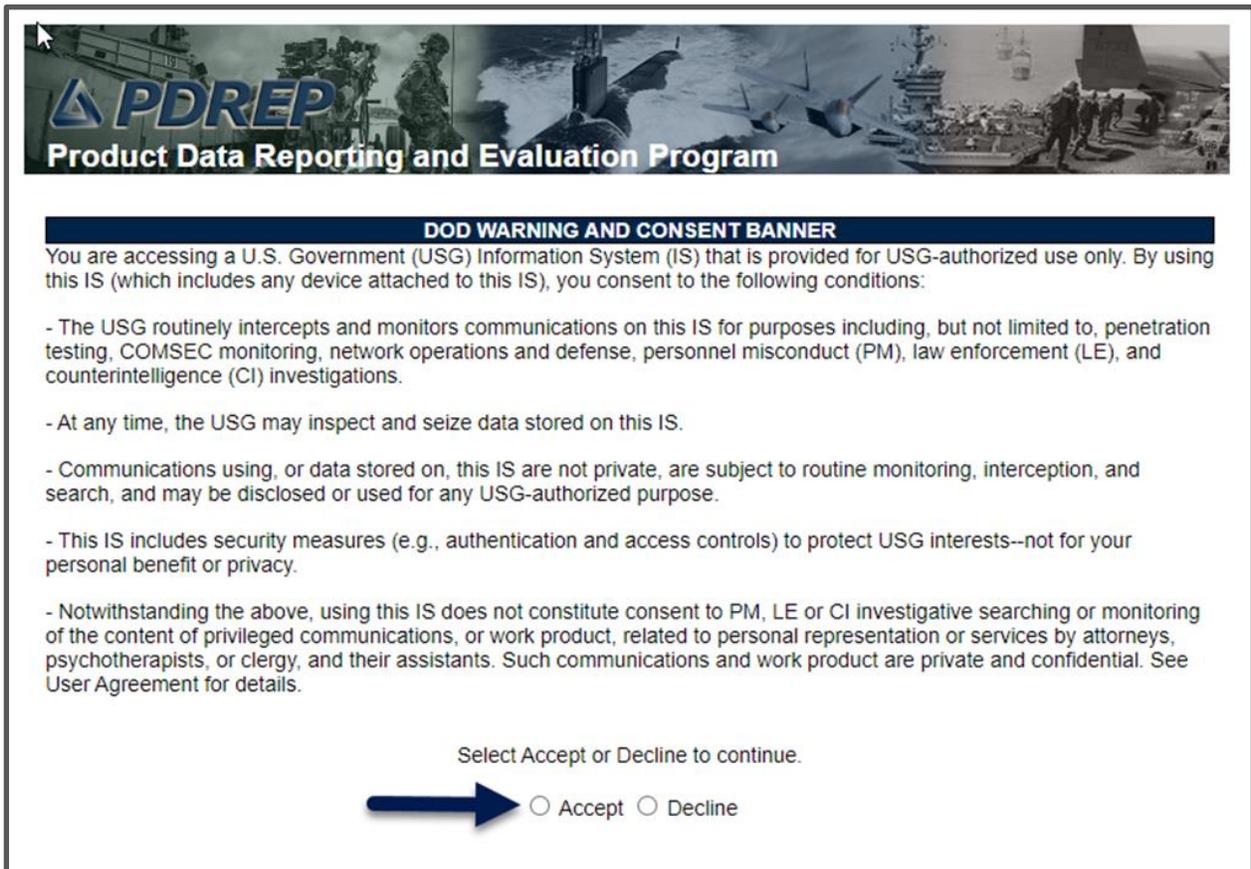


Figure 6.2

- Select Accept. Selecting Decline will stop the process and return user to previous screen.
- Browser will navigate to display only version of SAAR-P

6.2 Enter Background Information

- Review User information and Contract information for personnel identification.
- Verifier enters/updates Security Manager Data Required (See **Figure 6.3**):
 - Type of Investigation (Mandatory) - The submitter’s last type of background investigation (i.e., Tier 3, Tier 5, etc.).
 - Date of Investigation (Mandatory) - Date of submitters last investigation (above). Select date from calendar icon or enter manually using MM/DD/YYYY format.
 - CE Deferred Investigation (Mandatory) - Enter yes/no to validate whether or not the submitter is currently enrolled for “Deferred Investigation” in the Continuous Evaluation (CE) program.
 - CE Deferred Investigation Date (Conditionally Mandatory) - Date of submitters CE enrollment. Leave blank if user is not enrolled in CE. Select date from calendar icon or enter manually using MM/DD/YYYY format.
 - Access Level (Mandatory) - The access level granted to the user by the sponsoring agency/service (i.e. NA, Confidential, Secret, Top Secret, etc.).
 - Security Manager Email Address (Mandatory) – Should be pre-populated to the Security Manager or representative that initially received SAAR-P electronically. Update as needed.
 - Security Manager Name (Mandatory) - The Security Manager or representative enter his/her name to indicate that the above clearance and investigation information has been verified.
 - Security Manager Phone Number (Mandatory) - Security Manager’s telephone number.

Security Manager Data Required	
(M) Type of Investigation:	Tier 5
(M) Date of Investigation:	01/01/2020
CE Deferred Investigation:	NO
CE Deferred Investigation Date:	
(M) Access Level:	SECRET
(M) Security Manager Email Address:	SECURITY.MANAGER.CIV@MAIL.MIL
(M) Security Manager Name:	SECURITY MANAGER
(M) Security Manager Phone Number:	888 555-1212

Figure 6.3

- Verifier validates Signatures/dates of submitter and approver (See **Figure 6.4**).

Signatures			
Submitter Date:	09/19/2023	Signature:	CONTRACTOR.SUPPORT.1234567890
Approver Date:	09/20/2023	Signature:	APPROVER.SUPERVISOR.SPONSOR.9876543210
Verifier Date:		Signature:	

Figure 6.4

- Verifier enters comments that will be included in the notification to submitter. This is OPTIONAL for Verify but MANDATORY for Reject (See **Figure 6.5**).

(CM) Approver Comments (will be appended to email sent to user)

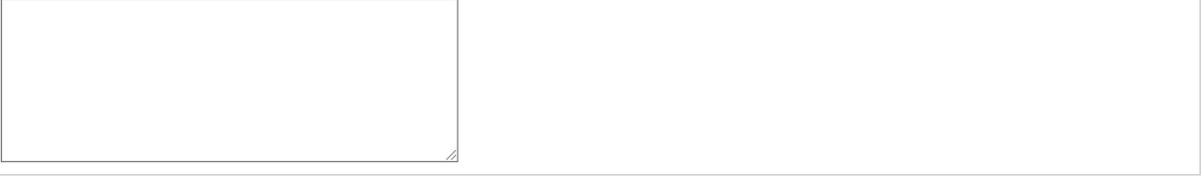


Figure 6.5

6.3 Verifying or Rejecting SAAR-P

Verifier verifies/rejects SAAR-P (See **Figure 6.6**):



Figure 6.6

To verify SAAR-P, select 'Verify and Sign'.

- Verifier’s browser will be navigated to a confirmation screen (See **Figure 6.7**).
- Requester is notified of Security Managers verification (See **Appendix 1 – Notifications**).

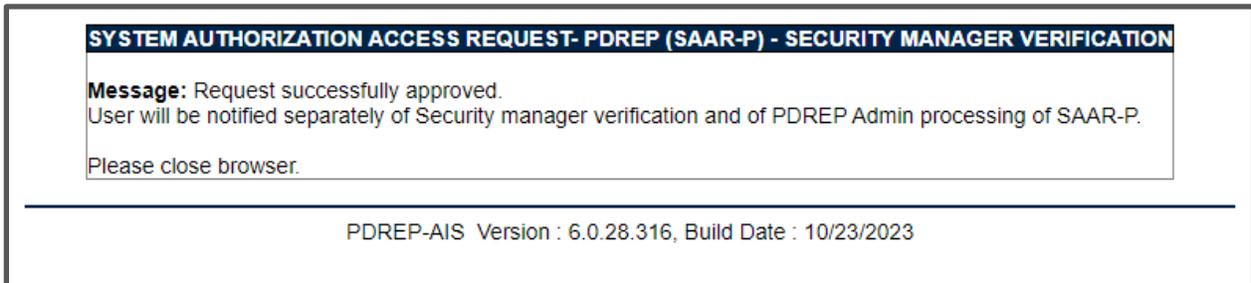


Figure 6.7

NOTE: When selecting “Verify and Sign” verifier is *DIGITALLY SIGNING* that they have verified all the information as outlined above and the SAAR-P will be digitally signed and stamped with verifier information from CAC/PIV/PKI certificate.

To reject a SAAR-P, select “Reject”

- Verifier’s browser will be navigated to a confirmation screen (See **Figure 6.8**).
- Requester is notified of Security Managers rejection (See **Appendix 1 – Notifications**).

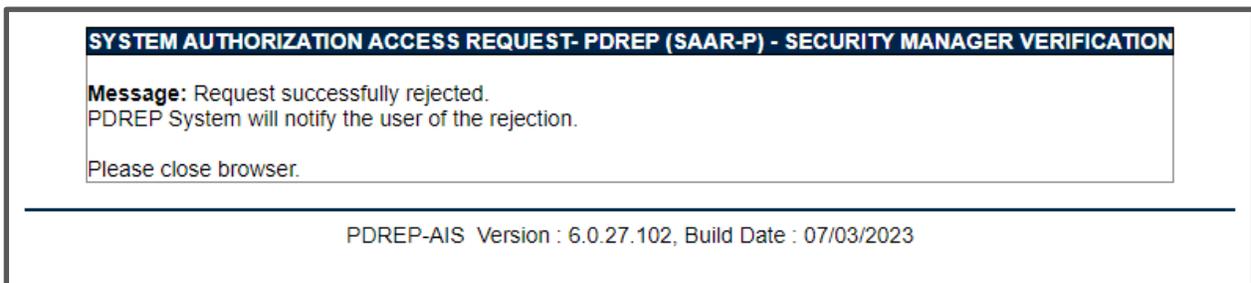


Figure 6.8

7 PROCESSING THE SAAR-P (PDREP ADMIN)

- PDREP-AIS Admin audits SAAR-P. Refer to PDREP-AIS User Access Work Instructions.
 - PDREP Admin may deny request if request does not pass audit. Requester is notified of finding of Audit. (See **Appendix 1** – Notifications).
 - PDREP Admin may reduce accesses requested, if requester/DoDAAC is not authorized.
 - PDREP Admin may send additional requests for information as required:
 - Contract not found in FPDS-NG.
 - Supervisor and Security Manager are same.
 - Submitter and Security Manager are same.
 - Insufficient initial justification.
 - Notations of audits are entered in justification box.
- PDREP Admin waits for all POC e-mails for additional permissions.
- SAAR-P is in hold status until all secondary approvals are received.
 - Accesses may be altered/removed based on POC replies.
- PDREP Admin will process SAAR-P. User is notified the account has been processed (See **Appendix 1** – Notifications).

8 PDREP LOGIN

8.1 Initial Login (Synchronizing Account with CAC/PIV/Cert)

In order to access the PDREP-AIS, a User Account must be created and a User Name and Password obtained. User accounts are established by submitting a SAAR-P which are eventually processed by a PDREP Admin.

When processed, NEW SAAR-P notifications will contain a USER ID and how to obtain a temporary password (See **Appendix 1** – Notifications).

Contrary to most users' memories who state they have "always" logged in with CAC/PIN, it is impossible to login initially with CAC/PIN as the hash code from your CAC has not been synchronized with your PDREP-AIS account yet.

To login the first time:

- Access the Product Data Reporting and Evaluation Program web page located at the following <https://www.pdrep.csd.disa.mil> (See **Figure 8.1**).

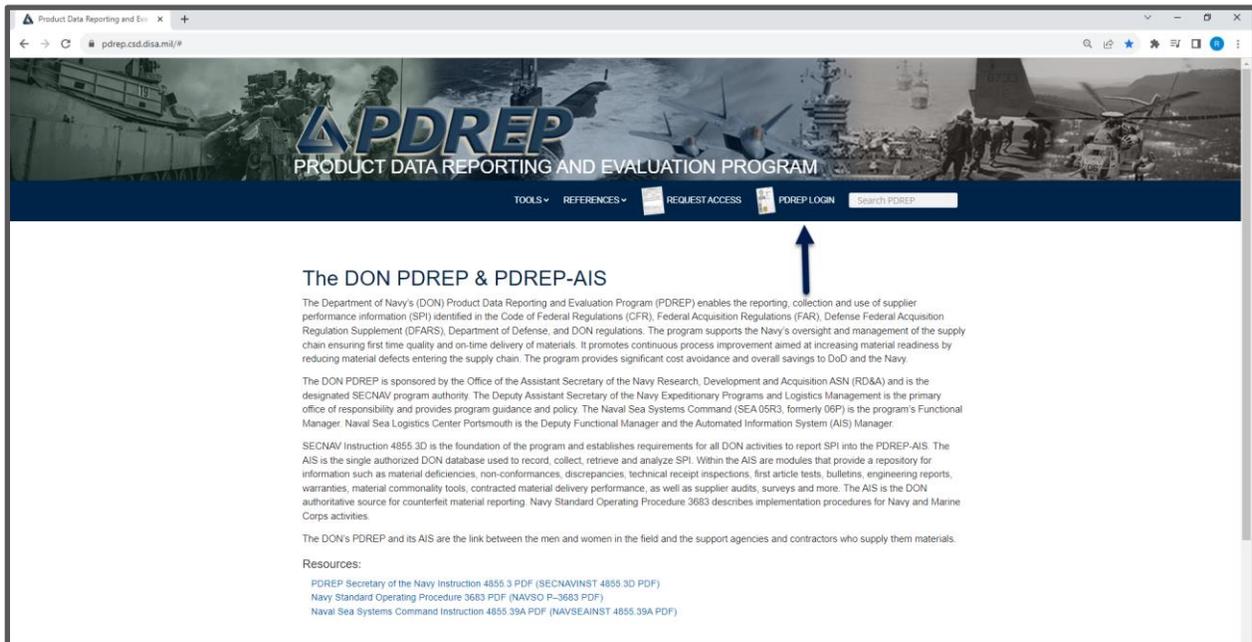


Figure 8.1

- Select 'PDREP LOGIN'.
- User may need to select certificate (See **Figure 8.2a**).
- User may need to enter CAC/PIV/Certificate PIN (See **Figure 8.2b**).

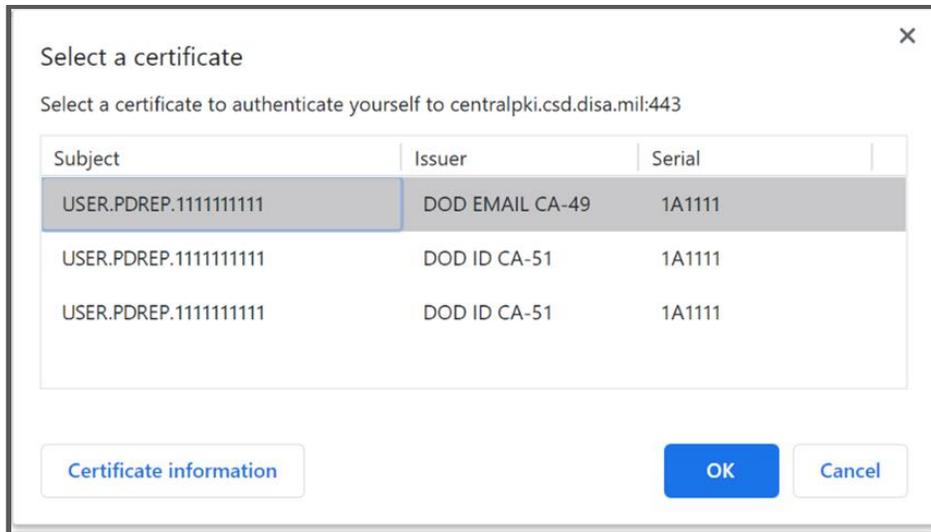


Figure 8.2a

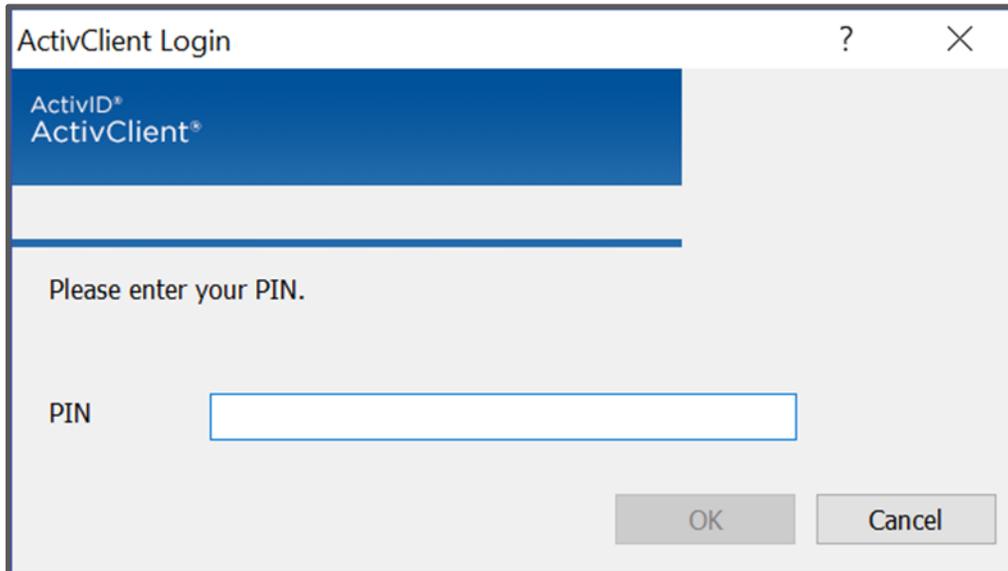


Figure 8.2b

- Browser will navigate to DOD WARNING AND CONSENT BANNER ((See Error! Reference source not found.3).

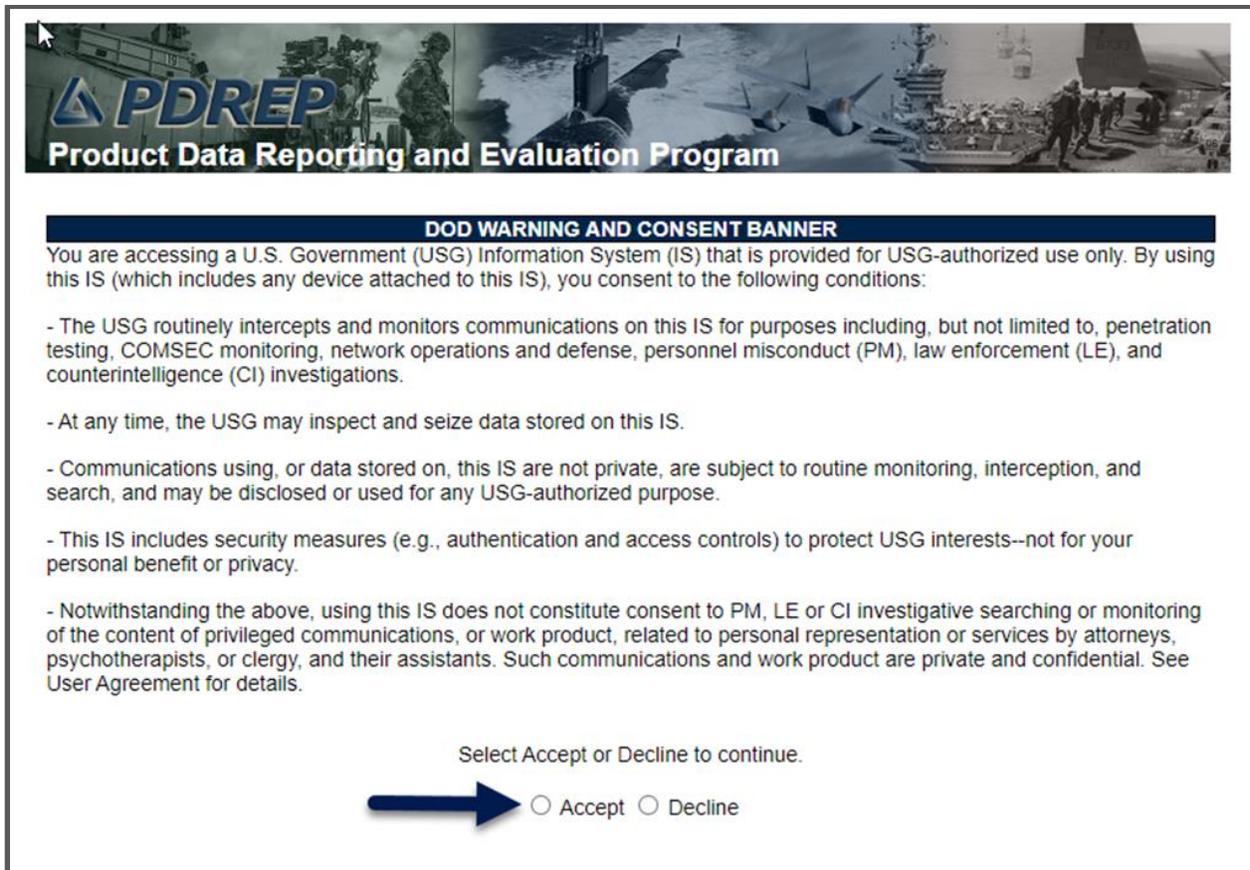


Figure 8.3

- Select Accept. Selecting Decline will stop the process and return user to previous screen.
- Browser will then be navigated to 'PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP) – LOGIN' screen (See Error! Reference source not found.4).
 - It is not necessary to enter 'USER ID' or 'Password' (See Error! Reference source not found.4, Item 1).
- Select 'Forgot Password?' (See Error! Reference source not found.4, Item 2).

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP) - LOGIN

Instructions
 1. Enter User ID and Password
 2. Click Login
 3. If you do not remember the Password, click [Forgot Password?](#) link

User ID:

Password: [Forgot Password?](#)

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.4

- Browser will then be navigated to 'FORGOT PASSWORD' screen (See **Figure 8.5**).

FORGOT PASSWORD

Instructions
 1. Enter User ID and Email Address.
 2. Click Verify.

User ID:

Email Address:

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.5

- Enter your USER ID.
- Enter your e-mail address.
- Select 'Verify'. This will check the PDREP-AIS database for an active account with the USER ID/e-mail address.
- User screen will show verification with a link to PDREP Login (See **Figure 8.6**).
- User will also receive an automated e-mail with a temporary password and a link to PDREP HOME.
 - If user selects link to PDREP HOME from the email instead of the link on the Forgot Password page, your browser will navigate to PDREP web page.
 - User will need to select PDREP LOGIN.

- Browser will navigate to User ID/Password Login page (See **Figure 8.4**).

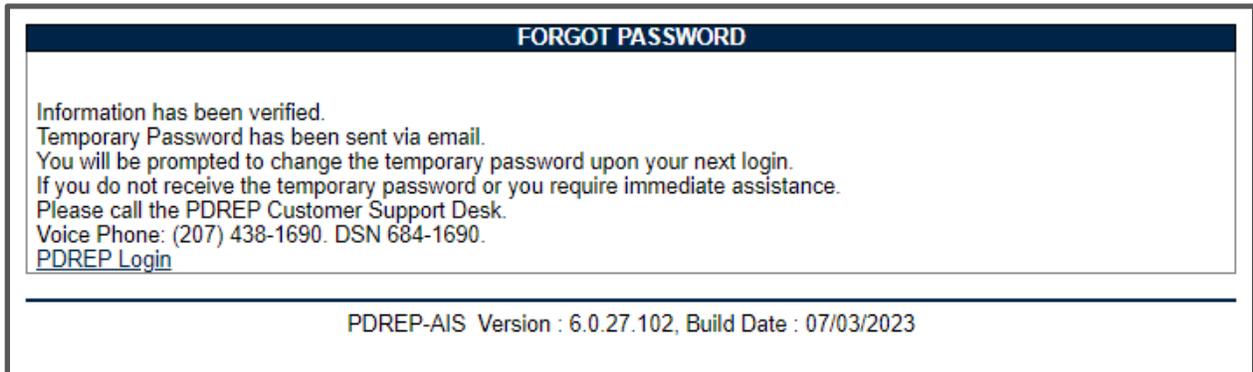


Figure 8.6

- Selecting PDREP Login will navigate browser to PDREP Login Screen (See **Figure 8.7**).

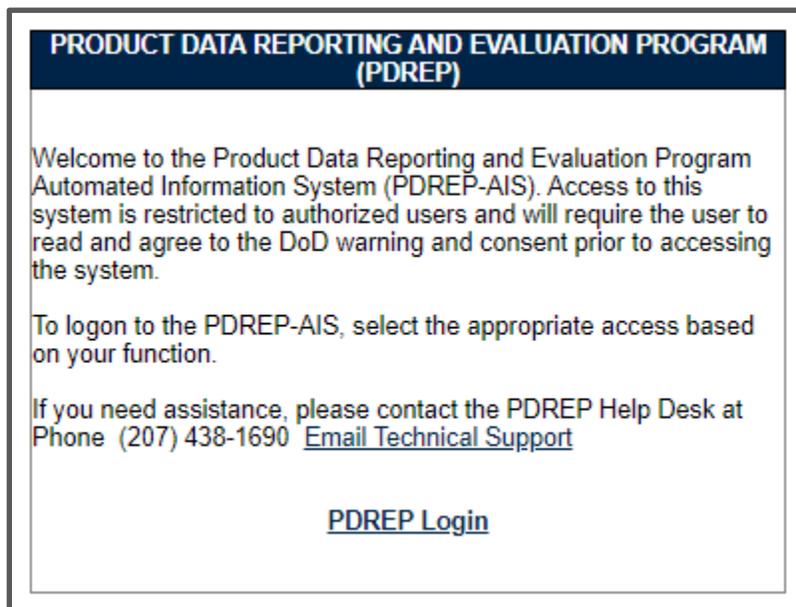


Figure 8.7

- Select PDREP Login
- Browser will Navigate to User ID/Password Login page (See **Figure 8.8**).

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP) - LOGIN

Instructions
 1. Enter User ID and Password
 2. Click **Login**
 3. If you do not remember the Password, click [Forgot Password?](#) link

1 → User ID:
 Password: [Forgot Password?](#)
2

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.8

- Enter User ID and Password (from automated e-mail).
- Select Login.
- Browser navigates to change password screen (See **Figure 8.9**).

CHANGE PASSWORD

Instructions
 1. - must be 15-20 characters
 2. - must contain at least two upper and lower case letters
 3. - must contain at least two numbers
 4. - must contain at least two special characters
 5. - cannot reuse your last 10 passwords
 6. - must differ from previous password by at least four characters
 7. - must not contain personal information such as:
 names, phone numbers, account names, birthdates, or dictionary words

Current Password:
 New Password:
 Confirm New Password:

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.9

- Reenter Current Password from e-mail.
- Create and enter New Password.
- Reenter New Password in Confirm New Password field.
- Select Save Password.

NOTE: Both Current and New Passwords are one-time usage only. Once you select Save Password, your CAC is synchronized with your PDREP-AIS account and passwords become obsolete.

NOTE: At this point, User has synchronized their CAC(Cert)/PIN with their PDREP-AIS Account and subsequent logins will only require CAC(Cert)/PIN until such time that their account becomes deactivated or they get a new CAC(Cert).

- Browser navigates to PDREP Message page (See **Figure 8.10**).

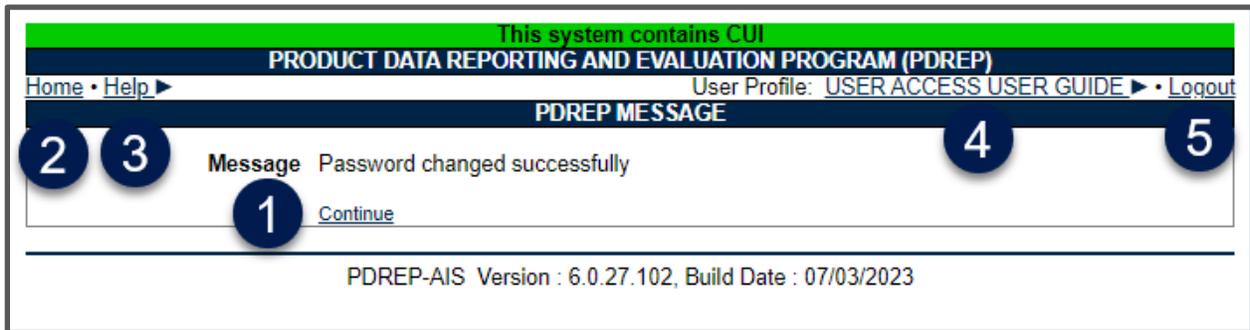


Figure 8.10

- Select Continue (See **Figure 8.10**, Item 1).
- This will navigate user to PDREP-AIS Home page (See **Figure 8.11**).

NOTE: At this point, User has successfully logged in to PDREP-AIS and may use any modules that they have access.

- Other Items that will also be on all other PDREP-AIS pages:
 - Selecting “Home” from anywhere in PDREP-AIS will return user to the PDREP-AIS home page.
 - Hover over “Help” to initiate a Fly out menu of help items (See **Figure 8.10**, Item 3). This is covered in **Section 9**.
 - Hover over “User Profile” on Home page or [YOUR NAME] on any other page to initiate a fly out menu to assist in user profile items (See **Figure 8.10**, Item 4). This is covered in **Section 10**.
 - Select “Logout” to logout of the system and browser will navigate to logout screen (See **Figure 8.10**, Item 5).

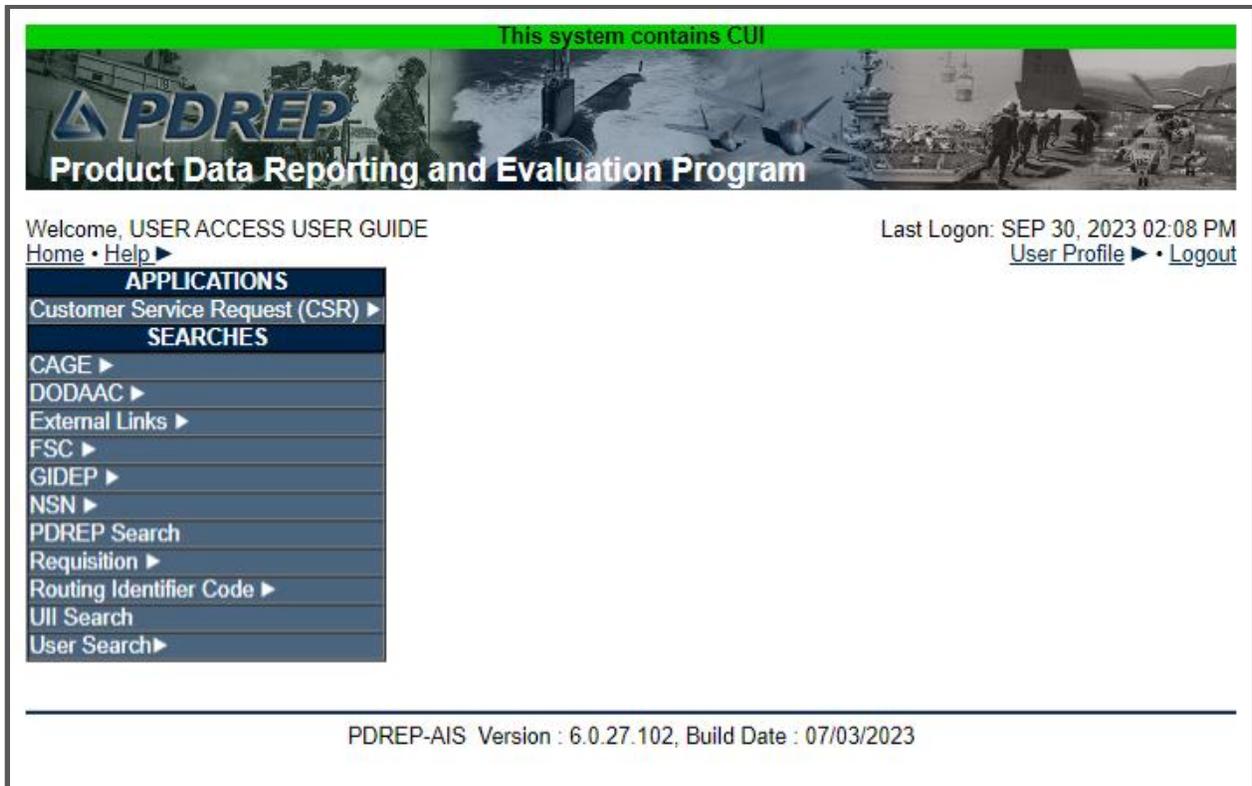


Figure 8.11

- When user selects “Logout”, browser is navigated to logout screen (See **Figure 8.12**).



Figure 8.12

- User may either:
 - Login to PDREP-AIS again (See **Figure 8.10, Item 1**).
 - Close Browser (See **Figure 8.10, Item 2**).

8.2 Follow-on Login

- Navigate Browser to PDREP-AIS Web page and select PDREP LOGIN (See **Figure 8.13**).

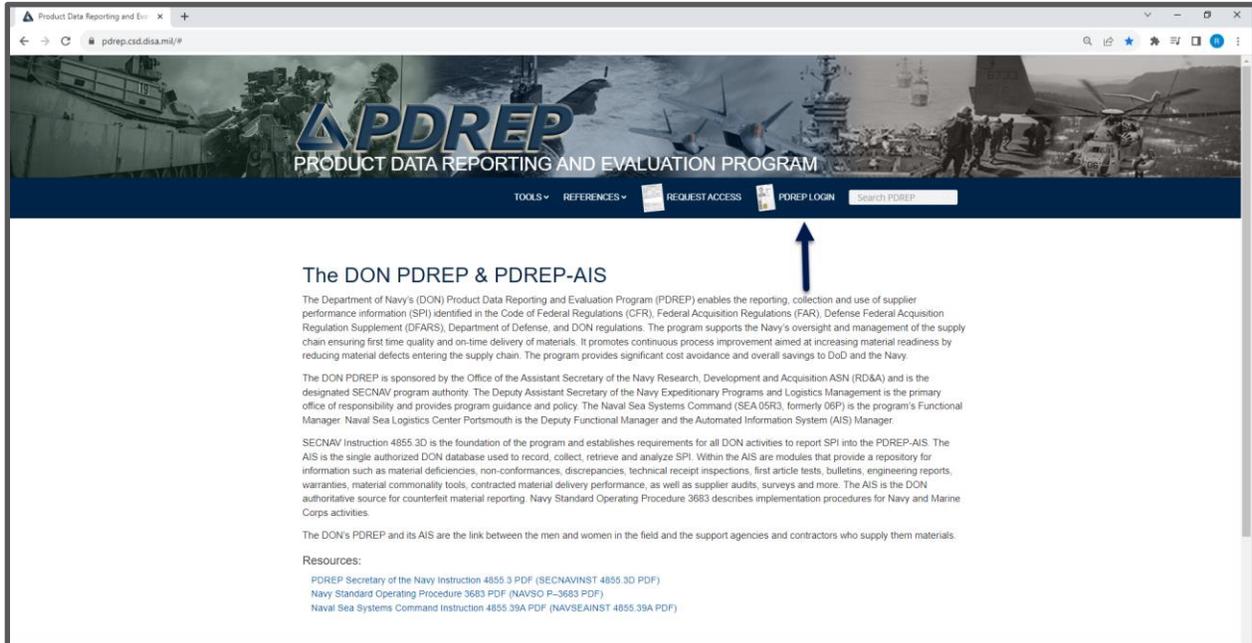


Figure 8.13

- User may need to select a certificate if not cached in their browser and enter CAC/PIV/Certificate PIN.
- Browser navigates to DOD WARNING AND CONSENT BANNER (See **Figure 8.14**).
 - Selecting accept will navigate to PDREP-AIS Home Page unless user has selected a default application. This is covered in **Section 10**.
 - Selecting Decline will navigate back to PDREP-AIS Web page.

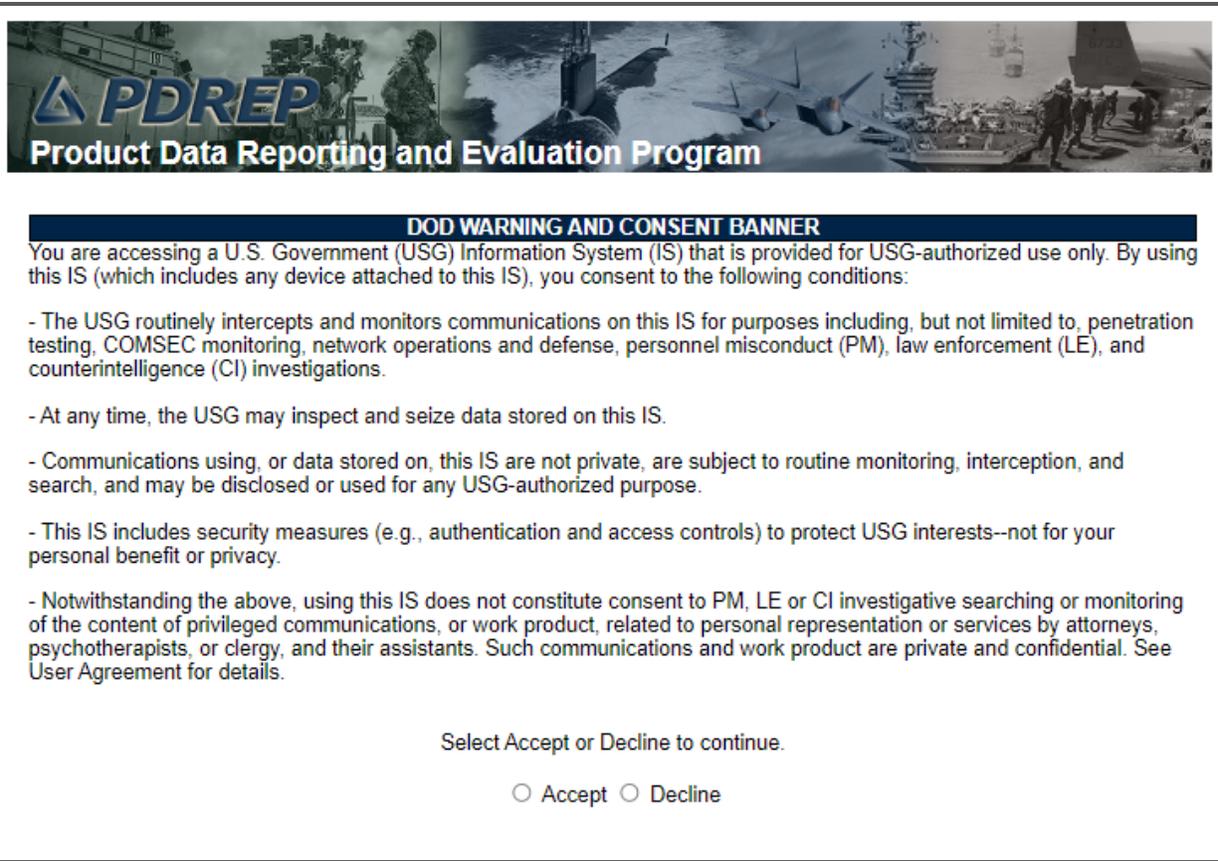


Figure 8.14

- Browser navigates to PDREP Home page (See **Figure 8.15**).
 - Selecting “Home” from anywhere in PDREP-AIS will return user to this page.
 - Hover over “Help” to initiate a Fly out menu of help items (See **Figure 8.8**, Item 3). This is covered in **Section 9**.
 - Hover over “User Profile” on Home page or [YOUR NAME] on any other page to initiate a fly out menu to assist in user profile items (See **Figure 8.8**, Item 4). This is covered in **Section 10**.
 - Select “Logout” to logout of the system and browser will navigate to logout screen (See **Figure 8.8**, Item 5).
 - Left Menu will display available applications, searches and reports. end on what modules user has been approved.
 - Table will display Recently Accessed Record(s) if applicable for records accessed in the last 24 hours.

This system contains CUI



Welcome, USER ACCESS USER GUIDE Last Logon: OCT 02, 2023 06:25 AM
[Home](#) • [Help](#) [User Profile](#) • [Logout](#)

APPLICATIONS	Recently Accessed Record(s)		
Customer Service Request (CSR) ▶	Record Type	Record Control Number	Last Accessed Date/Time
Product Quality Deficiency Report (PQDR)▶	QDR	DODAAC-23-1234 (View/Edit)	2023-10-02 08:21:17.0
SEARCHES			
CAGE ▶			
DODAAC ▶			
External Links ▶			
FSC ▶			
GIDEP ▶			
NSN ▶			
PDREP Search			
Requisition ▶			
Routing Identifier Code ▶			
Ull Search			
User Search▶			

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.15

8.3 Login Failures

If browser navigates to the USER ID/PASSWORD page it is because the database cannot not find an active account synchronized to your CAC (See **Figure 8.16**). The most common reasons are:

- Your NEW/RENEW SAAR-P has just been processed and you were directed to this page. Continue as directed.
- Your account has been disabled. You have not logged into PDREP-AIS in the last 30 to 45 days. Use “Forgot Password?” link to re-enable account.
- Your account was deactivated. You have not logged into PDREP-AIS in over 45 days or your contract has expired. You will not be able to use this page to reset your password. You will need to resubmit a SAAR-P. You will encounter an error if you use the forgot password page (See **Figure 8.17**).
- You have a new CAC/PIV/Cert and need to resynchronize your CAC. Contact the NSLC Portsmouth Help Desk to clear you hash code.
- The system/network is down. Contact NSLC Portsmouth Help Desk to verify system is operational.

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP) - LOGIN

Instructions
1. Enter User ID and Password
2. Click Login
3. If you do not remember the Password, click [Forgot Password? link](#)

User ID:

Password: [Forgot Password?](#)

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.16

FORGOT PASSWORD

Instructions
1. Enter User ID and Email Address.
2. Click Verify.

- Unable to verify User ID and Email Address entered.
Please call the PDREP Customer Support Desk for further assistance.
Voice Phone: (207) 438-1690. DSN 684-1690.

User ID:

Email Address:

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 8.17

NOTE: *This is the error message received when network/system is down or when user account has been deactivated. Contact NSLC Portsmouth Help Desk to verify system is operational.*

9 PDREP HELP

Hovering over “Help” will create a Fly out menu with the following Items (See **Figure 9.1**):

- “Contact Help Desk with comment, question or feedback” will generate an e-mail to NSLC Portsmouth Help Desk, a shared resource between CPARS, SPRS and PDREP-AIS, so for faster assistance ensure you identify you ticket as PDREP-AIS.
- “Make a User Access or User Account Change” will navigate user to UPDATE SAAR-P (covered in **Section 10.5**).
- “View the user guides for help” will navigate browser to the “Guides and Manuals” page where users may find this and other user guides for each of the PDREP modules.
- “View the FAQs to see if the answer to my question is there” will navigate browser to FAQs page where many of the users may find answers in not already in the user guide.
- “Suggest a change to software or report a problem with the website” will navigate browser to the Customer Service Request (CSR) page.

The screenshot displays the PDREP-AIS user interface. At the top, a green banner reads "This system contains CUI". Below it is a header with the PDREP logo and the text "Product Data Reporting and Evaluation Program". The main content area shows a welcome message "Welcome, USER ACCESS USER GUIDE" and the text "Last Logon: OCT 03, 2023 06:14 AM". A navigation bar includes "Home" and "Help" (with a flyout menu open). The flyout menu items are numbered 1 through 5:

1. Contact Help Desk with comment, question, or feedback
2. Make a User Access or User Account Change
3. View the user guides for help
4. View the FAQs to see if the answer to my question is there
5. Suggest a change to software or report a problem with the website

Other navigation items include "Customer Service", "SEA", "CAGE", "DODAAC", "External Links", "FSC", "GIDEP", "NSN", "PDREP Search", "Requisition", "Routing Identifie", "UII Search", and "User Search". The footer displays "PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023".

Figure 9.1

10 USER PROFILE

To view or update your User Profile, hover over 'User Profile' on the top right of the PDREP-AIS Home page or [YOUR NAME] on any other page to display the fly out menu (See **Figure 10.1**).

The screenshot displays the PDREP-AIS user interface. At the top, a green banner reads "This system contains CUI". Below this is the PDREP logo and the title "Product Data Reporting and Evaluation Program". The main content area includes a welcome message, navigation links, and a list of applications and searches. On the right, the user's name and last login time are displayed, along with a flyout menu for the user profile. Five numbered arrows point to the menu items: 1 points to "View Profile", 2 to "Edit Profile", 3 to "Edit Distribution List", 4 to "Edit Point of Contacts", and 5 to "Access Change Request".

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.1

10.1 Viewing Your User Profile

To View your User Profile:

- Select “View Profile” from fly out menu (See **Figure 10.1**, Item 1).
- Browser will navigate to User Profile – View page.
- User can print the page for reference by selecting the Print button (See **Figure 10.2**, Item 1).
- User can navigate to previous page by selecting the Back button (See **Figure 10.2**, Item 2).
- User can review the following information:
 - User Profile (See **Figure 10.2**, Item 3).
 - Email Distribution List (See **Figure 10.2**, Item 4).
 - Points of contact (See **Figure 10.2**, Item 5).
- User can update some information by selection “Click here” link (See **Figure 10.2**, Item 6) and browser will navigate to User Profile – Edit Page (See **Section 10.2**).

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

Home • Help User Profile: USER ACCESS USER GUIDE • Logout

1 Print Back 2

3 USER PROFILE - VIEW

To update information [Click here](#) 6

Name: USER ACCESS USER GUIDE
 Title: USER ACCESS
 P.O.Box:
 Address: 123 MAIN STREET
 City/State/Zip: ANY TOWN STATE 12345-6789
 Country: UNITED STATES
 Phone: 888-555-1212
 DSN Phone:
 Email Address: user.access.user.guide.civ@mail.mil
 Organization Code:
 Logo: 0
 SubjectCN: USER GUIDE.USER ACCESS.1234567890

4

5

4 Email Distribution List

Email Address	Name	List Name
john.lennon@us.navy.mil	John Lennon	Beatles
george.harrison@us.navy.mil	George Harrison	Beatles
richard.starkey@us.navy.mil	Ringo Starr	Beatles
james.paul.mccartney@us.navy.mil	Paul McCartney	Beatles

Point of contact record count: 1

5

Point of contact

Name	Email Address	Activity/Organization	Contact Type	Phone
GOVERNMENT EMPLOYEE	GOVERNMENT.EMPLOYEE@MAIL.MIL	ACTIVITY NAME	GOVERNMENT	123-456-7890

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.2

10.2 Editing Your User Profile

To edit your user profile:

- Select “Edit Profile” from fly out menu (See **Figure 10.1**, Item 1) or “Click here” link (See **Figure 10.2**, Item 6) and browser will navigate to User Profile – Edit Page (See **Figure 10.3**).

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

Home • Help ▶ User Profile: [USER ACCESS USER GUIDE](#) ▶ • Logout

User Information | Distribution Lists | Points of Contact | Access Change Request

User Profile - Edit

Instructions
(M) denotes a mandatory field
1. Enter mandatory fields
2. Enter known optional fields
3. To update User Profile, click Save
Changing Profile data will not update previously saved records

User ID: UGUID

(M) First Name: FIRST (M) Last Name: LAST

Title: TITLE

P.O.Box:
Address: 123 MAIN STREET

(M) City: ANY TOWN

State/Province: STATE Zip/Postal Code: 03804-5000

Country: UNITED STATES

(M) Area Code: 888 (M) Work Phone Number: 555 — 1212 Extension:

International Phone Number

DSN Telephone Number: 123-4567

Email Address: user.email.civ@mail.mil
Please contact NSLC help desk if you need to change your email address.

(M) Supervisor Email Address: supervisor.email.civ@mail.mil

Organization Code: ORG CODE

Logo: --Select--

Default Application: Home (Default)

Save Cancel

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.3

- Update the following as needed:
 - Name.
 - Title.
 - Commercial Phone Number.
 - DSN Phone Number.

- Supervisor e-mail address.
- Organization Code.
- Logo (to be placed on correspondence letters).
- Default Application – This allows users to by-pass the PDREP-AIS Home page when logging in and navigates directly to applicable screen of choice in a module user has already been approved.

NOTE: DCMA users need to submit an Access Change Request to update Organization Code (Team Code) or Supervisor E-mail address.

- Select the Save button to retain changes. Selecting Cancel returns user to User Profile – View page.
- Browser navigates to confirmation message page (See **Figure 10.4**).

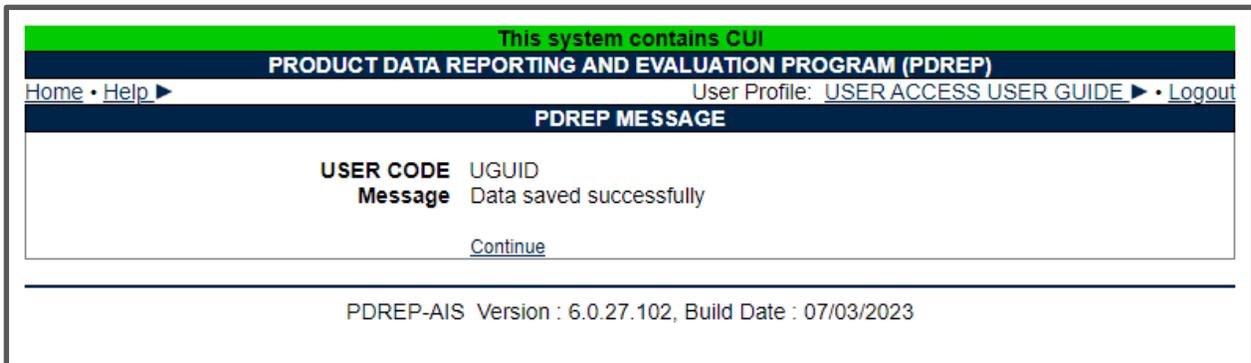


Figure 10.4

- Select Continue to navigate back to User Profile – View page.

10.3 Creating and Editing Distribution Lists

The Distribution List tab contains any e-mail addresses that you might use on distribution lists for PDREP messages. Distribution lists are used in PDREP forwarding messages, e-mail messages, and letters. In most PDREP applications Distribution lists will show near the end of the CC drop down list (see **Figure 10.5** and **Figure 10.6**).

NOTE: *The User bears the responsibility to ensure data distributed from PDREP-AIS is on a need to know basis and that data, e-mails, and attachments are marked with appropriate classification and distribution.*

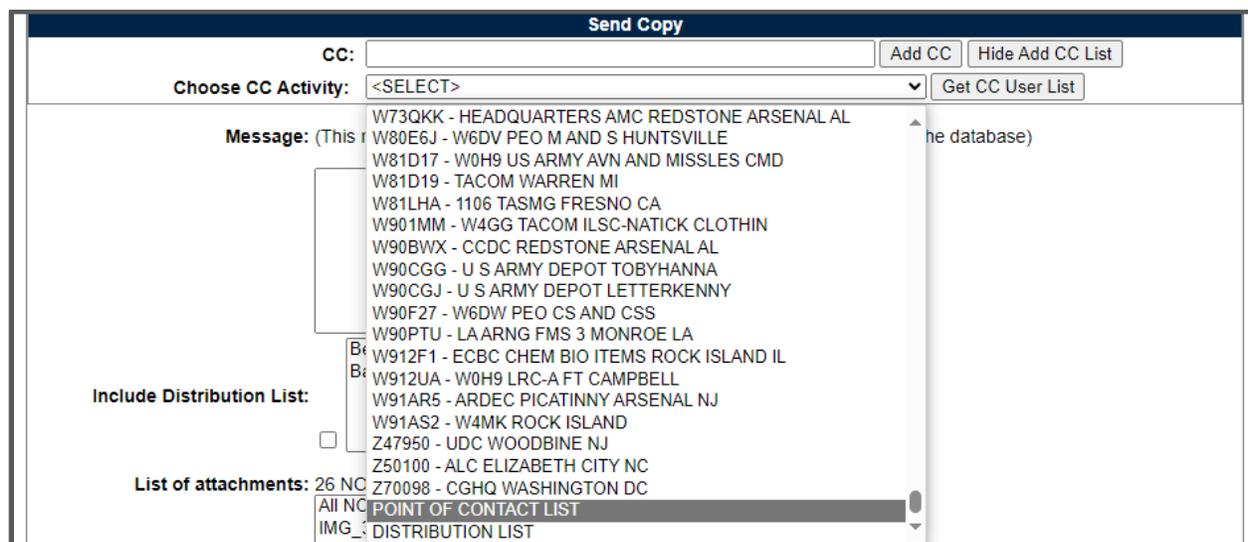


Figure 10.5

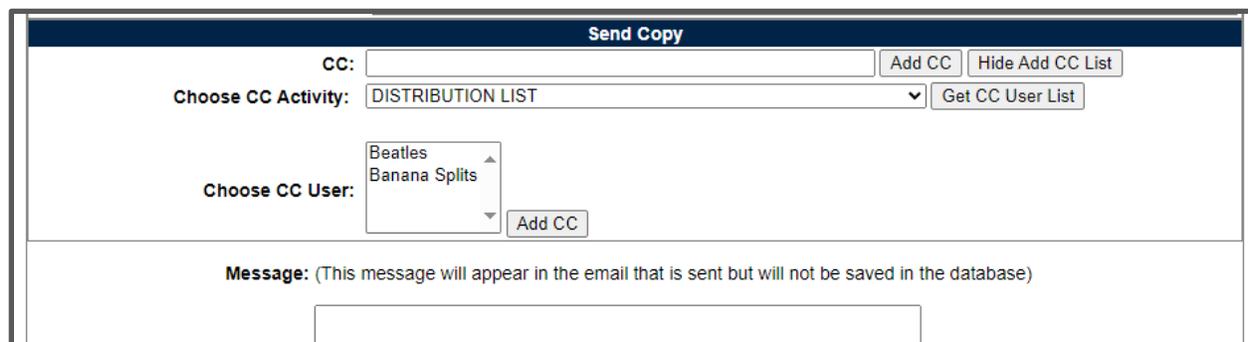


Figure 10.6

- To access Distribution tab either:
 - Select tab if already in the user profile section.

- Select Edit Distribution List from the fly out menu (See **Figure 10.1**, Item 1).
- Browser navigates to Create Distribution List page (See **Figure 10.7**).

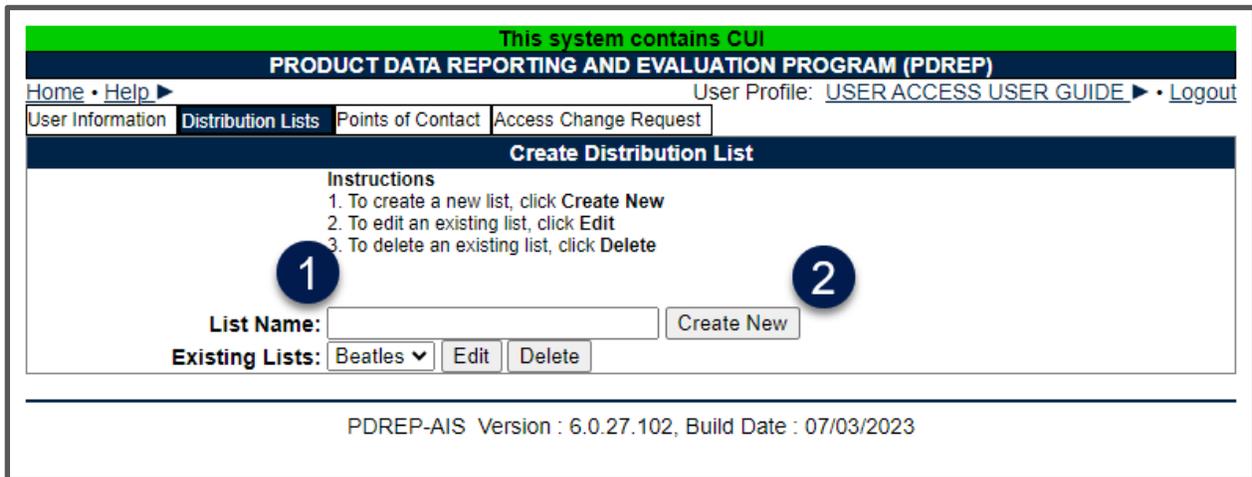


Figure 10.7

- To Create a Distribution List:
 - Enter a List Name.
 - Select Create New button.
 - List is Created.
- To Edit list (See **Figure 10.8**):
 - Select list from Existing Lists DDL.
 - Select Edit.

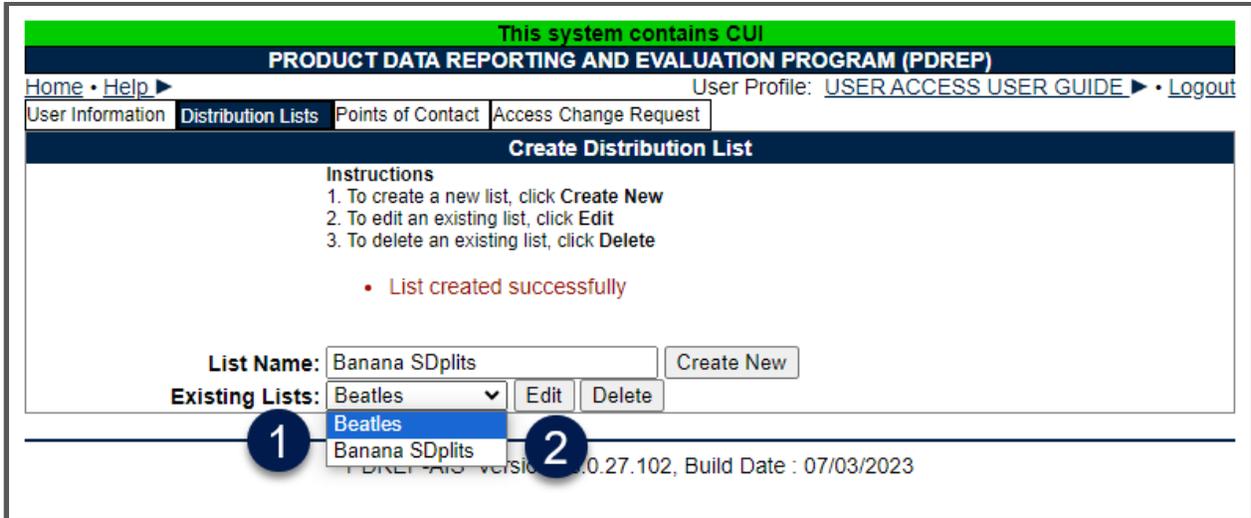


Figure 10.8

- Browser navigates to Edit Distribution List page list (See Figure 10.9):

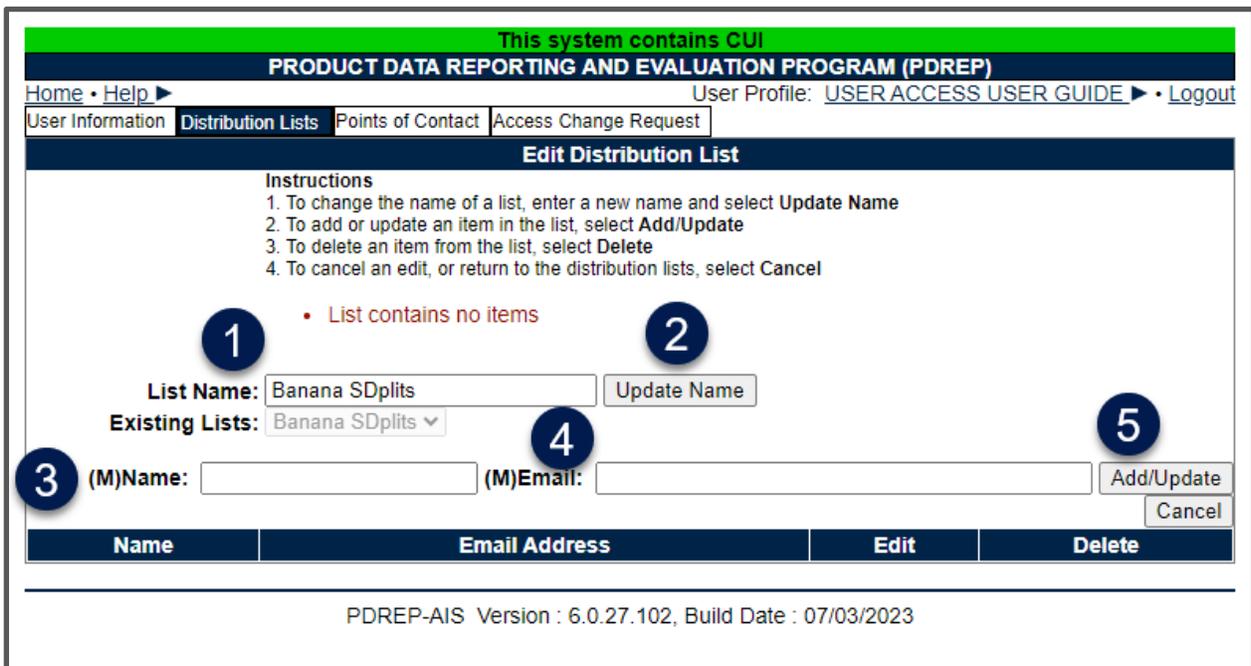


Figure 10.9

- List Name can be edited by:
 - Editing Name in List Name.
 - Selecting Update Name button.

- Items can be added to list by:
 - Entering Name.
 - Entering Email.
 - Selecting Add/Update button.

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

[Home](#) • [Help](#) ▶ User Profile: [USER ACCESS USER GUIDE](#) ▶ • [Logout](#)

[User Information](#) | [Distribution Lists](#) | [Points of Contact](#) | [Access Change Request](#)

Edit Distribution List

Instructions

1. To change the name of a list, enter a new name and select **Update Name**
2. To add or update an item in the list, select **Add/Update**
3. To delete an item from the list, select **Delete**
4. To cancel an edit, or return to the distribution lists, select **Cancel**

List Name:

Existing Lists: ▼

(M)Name: **(M)Email:**

Name	Email Address	Edit	Delete
Drooper	drooper@banana.splits.com	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Snorky	snorky@banana.splits.com	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Chongo	chongo@banana.splits.com	<input type="button" value="Edit"/> 1	<input type="button" value="Delete"/> 2
Fleegle	fleegle@banana.splits.com	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.10

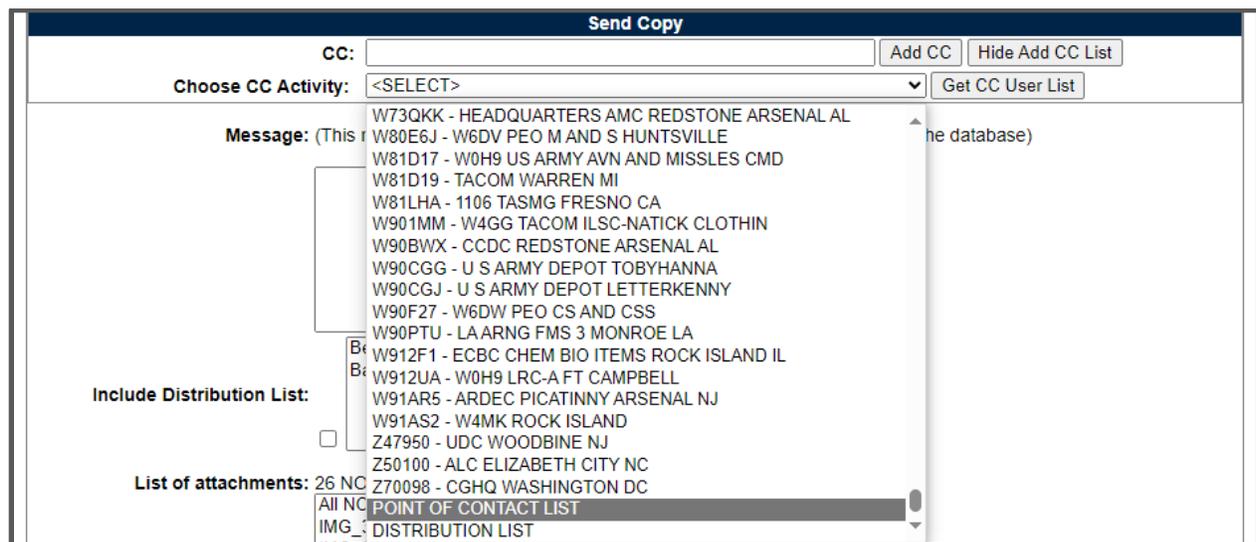
- Items on list can be modified by (See **Figure 10.10**):
 - Select the appropriate Edit button.
 - Item will appear above table.
 - Update name or email as needed.
 - Select Add/Update button.
- Items can be deleted by:
 - Selecting the appropriate Delete button
 - Selecting OK in the verification pop-up window

- Select Cancel to return to the Create Distribution List page.
- To Delete a Distribution list:
 - Ensure browser has navigated back to Create Distribution List page.
 - Select list from Existing Lists.
 - Select Delete button.

10.4 Creating and Editing Point of Contact (POC)

Points of Contact are used primarily used by PQDR Support Point or Action Point users for identifying Government, Contractor, or Supplier investigators but can also be used as a supplemental address list for all users. POCs are not the same as Distribution List members. In most PDREP applications, POCs lists will show near the end of the CC drop down list (See **Figure 10.11** and **Figure 10.12**).

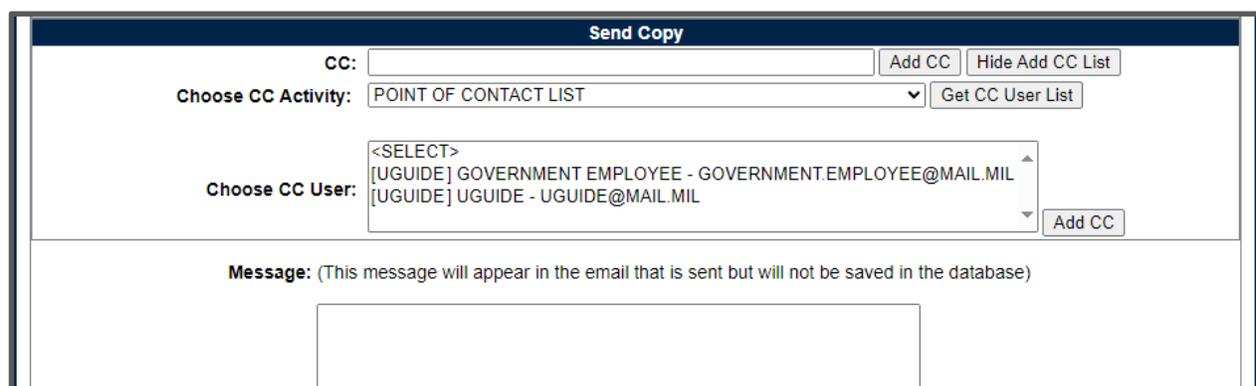
NOTE: *The User bears the responsibility to ensure data distributed from PDREP-AIS is on a need to know basis and that data, e-mails, and attachments are marked with appropriate classification and distribution.*



The screenshot shows the 'Send Copy' form with the following elements:

- CC:** A text input field, an 'Add CC' button, and a 'Hide Add CC List' button.
- Choose CC Activity:** A dropdown menu currently set to '<SELECT>', with a 'Get CC User List' button to its right.
- Message:** A text area containing the text: "ne database)".
- Include Distribution List:** A checkbox that is currently unchecked.
- List of attachments:** A list of 26 items, including "POINT OF CONTACT LIST" and "DISTRIBUTION LIST".

Figure 10.11



The screenshot shows the 'Send Copy' form with the following elements:

- CC:** A text input field, an 'Add CC' button, and a 'Hide Add CC List' button.
- Choose CC Activity:** A dropdown menu set to 'POINT OF CONTACT LIST', with a 'Get CC User List' button to its right.
- Choose CC User:** A dropdown menu showing three options: '<SELECT>', '[UGUIDE] GOVERNMENT EMPLOYEE - GOVERNMENT.EMPLOYEE@MAIL.MIL', and '[UGUIDE] UGUIDE - UGUIDE@MAIL.MIL'. An 'Add CC' button is located to the right of the dropdown.
- Message:** A text area containing the text: "(This message will appear in the email that is sent but will not be saved in the database)".

Figure 10.12

- To access the Add Point of Contact page, either:
 - Select "Edit Point of Contacts" from the User Profile fly out menu (See **Figure 10.1**, Item 4).

- Of if already in the User Profile module, select the Points of Contact tab.

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

Home • Help ► Maintenance Message User Profile: USER ACCESS USER GUIDE ► • Logout

User Information Distribution Lists **Points of Contact** Access Change Request

Add Point of Contact

Instructions

1. To add new Point of Contact, click **Add New POC**
2. Point of Contact (POC) filter instructions
 - a My POCs - only users POCs shown
 - b POCs my Activity - Filters by users activity
 - c All POCs - Filters all activities and cage codes assigned
3. Click **Cancel** to exit this screen

Point of Contact Filter: User's POCs ▼ Save Point of Contact Filter

Add New POC Cancel

Point of contact record count: 1

User Code	Name	Organization	Contact Type	Edit	Delete
[UGUIDE]	GOVERNMENT EMPLOYEE	ACTIVITY NAME	G	Edit	Delete

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.13

The Point of Contact Filter allow users to modify which users are displayed in the DDLs.

- To modify POC Filter (See **Figure 10.14**):
 - Select down arrow to display the filter options.
 - Select one of the following:
 - User's POCs – These are your POCs.
 - Primary Activity POCs – These are everyone's POCs that has your Primary DoDAAC.
 - Primary and Secondary Activities POCs – These are everyone's POCs that shares either your Primary DoDAAC or any of your Secondary DoDAACs.
 - Select Save Point of Contact Filter button. New POCs will display in table below (See **Figure 10.15**).

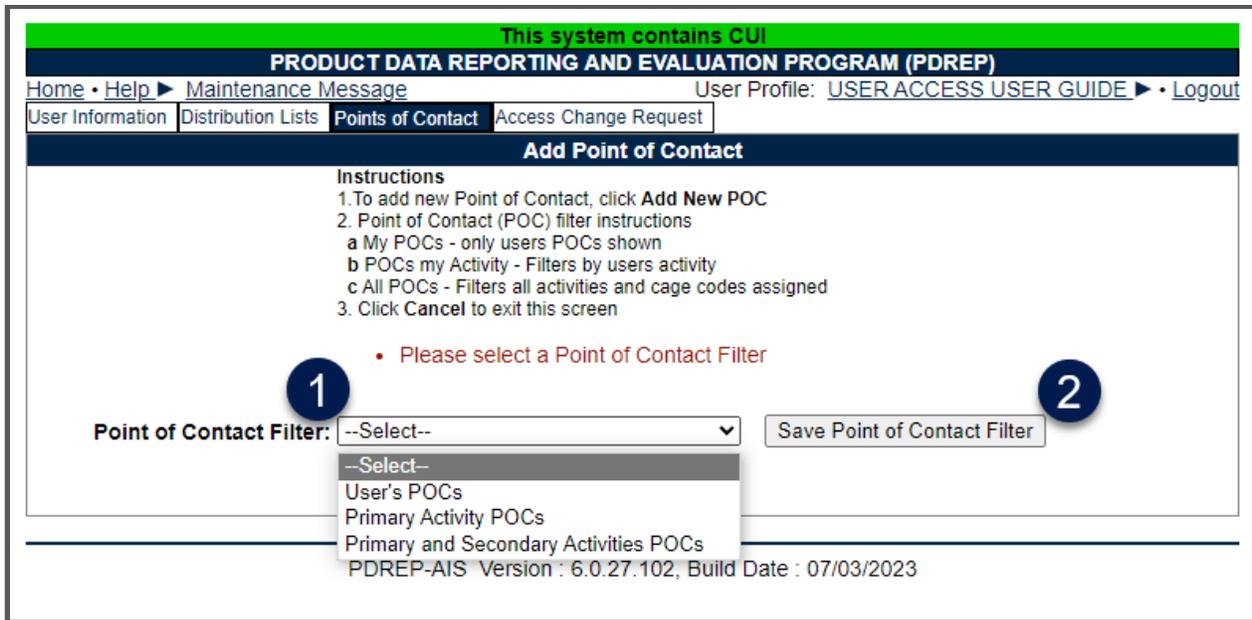


Figure 10.14

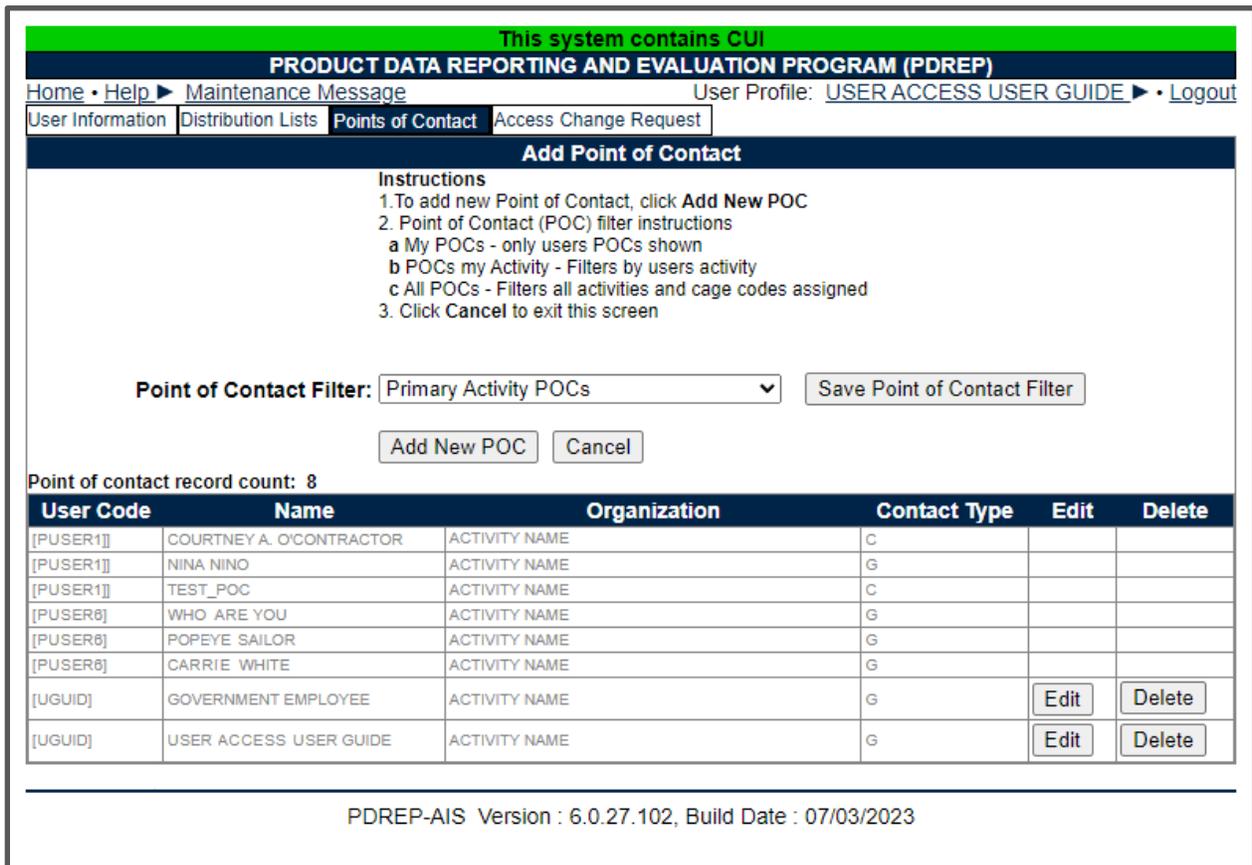


Figure 10.15

- To add another POC:
 - Select “Add New POC” button.
 - Browser navigates to “Add Point of Contact” screen (See **Figure 10.16**).

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

Home • Help ► Maintenance Message User Profile: USER ACCESS USER GUIDE ► • Logout

User Information | Distribution Lists | **Points of Contact** | Access Change Request

Add Point of Contact

Instructions
 1. Enter mandatory fields
 2. Enter known optional fields
 3. Enter DODAAC of Govt POC or CAGE Code of Contractor/Supplier POC
 4. Click **Save** to add to list
 5. Click **Cancel** to cancel the process

(M) POC Name:

(M) Contact Type: --Select-- ▼

Activity/Company Name:

DODAAC:

CAGE Code:

Address:

City:

State/Province: --Select-- ▼

Country: --Select-- ▼

Zip/Postal Code:

Phone Number:

Fax Number:

(M) Email Address:

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.16

- Complete fields as needed:
 - Name (Mandatory).
 - Contact type (Mandatory):
 - Government.
 - Contractor.
 - Supplier.
 - Activity/Company Name*.
 - DoDAAC.

- CAGE Code.
- Address*.
- City*.
- State/Province*.
- Country*.
- Zip Code*.
- Phone Number.
- Fax Number.
- E-mail Address (Mandatory).

NOTE: *By entering the DoDAAC or the CAGE Code and selecting the corresponding “Auto Fill” button, these fields will populate based on information already loaded in PDREP database from system(s) of record.

- Select Save (See **Figure 10.17**).

This system contains CUI

PRODUCT DATA REPORTING AND EVALUATION PROGRAM (PDREP)

[Home](#) • [Help](#) ► [Maintenance Message](#) User Profile: [USER ACCESS USER GUIDE](#) ► [Logout](#)

[User Information](#) | [Distribution Lists](#) | [Points of Contact](#) | [Access Change Request](#)

Add Point of Contact

Instructions

1. Enter mandatory fields
2. Enter known optional fields
3. Enter DODAAC of Govt POC or CAGE Code of Contractor/Supplier POC
4. Click **Save** to add to list
5. Click **Cancel** to cancel the process

• Saved Successfully

(M) POC Name:

(M) Contact Type:

Activity/Company Name:

DODAAC:

CAGE Code:

Address:

City:

State/Province:

Country:

Zip/Postal Code:

Phone Number:

Fax Number:

(M) Email Address:

Point of contact record count: 1

User Code	Name	Organization	Contact Type	Edit	Delete
[JGUID]	TEST POC	PRIMARY DODAAC	G	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

PDREP-AIS Version : 6.0.27.102, Build Date : 07/03/2023

Figure 10.17

- To edit a POC:
 - Select corresponding Edit button.
 - Browser will navigate to Edit Point of Contact page (same as add page with title change).
 - Update information.
 - Select save.
- To Delete POC:
 - Select corresponding Delete button.
 - Select OK on verification pop up window.
 - POC Deleted Successfully.

NOTE: **To Delete a POC not belonging to you, you must have Management Access at PQDR Support Point. Then Edit and Delete buttons will appear for all POCs for your Primary Activity.*

10.5 Submitting an Access Change Request

To request access to different applications in the PDREP-AIS, update DoDAACs, CAGES or to request different access privileges you currently have for an application, users will submit an access change request. The change request will parallel the same process for flow and notifications as when submitting original SAAR-P (Reference **Section 4**).

- To access the Access Change Request page, either:
 - Select “Access Change Request” from the User Profile fly out menu (See **Figure 10.1**, Item 5).
 - Of if already in the User Profile module, select the Access Change Request tab.
- Browser navigates to SAAR-P. Current User information, POCs, Contract information (for contractors), and accesses are defaulted on the SAAR-P.
- Update SAAR-P as needed:
 - Request/User Type:
 - Request Type is Defaulted to Update. There is also a Deactivate item in the DDL if needed.
 - User type is display only as a transition in user type requires a new account.
 - DoD Data Required:
 - Submitter Email Address is display only as this is a key field. If you need to update this, contact the NSLC Portsmouth Help Desk.
 - Supervisor/Sponsor Email Address.
 - Security Manager Email Address.
 - DoD Contract:
 - Contract Number.
 - Contract End Date.
 - CAGE Code.
 - Sponsor Phone Number.
 - Fax.
 - PDREP Reporting Tools accesses.
 - Re-enter citizenship and training confirmations.
 - Re-enter Justification for updates
- Submit SAAR-P

- Select read the agreement
- Browser navigated to User Agreement
- Read and scroll though user agreement.
- At the end of the user agreement (See Figure 4.16), select either:
 - 'I have read the agreement and agree to follow' which will navigate browser back to SAAR-P with a sign and submit button.
 - 'I do not agree' which will navigate browser back to SAAR-P.
- Select the 'Sign and Submit Request' button

NOTE: *Submitter is DIGITALLY SIGNING affirmation to the User Agreement and that all information on SAAR-P is correct. SAAR-P is stamped with user information from CAC/Cert.*

11 ACCOUNT DEACTIVATION

11.1 Active Accounts

Once users have synchronized their CAC/PIV/Cert with their account, the account is “Active”. In order for the account to remain active, users need to login at least once every 30 days since their last login.

After 23 days of not logging in, PDREP-AIS will send daily Inactivity notifications warning users to log in or the account will become disabled until the account is Disabled.

Users have 7 days from first notification to complete this task.

11.2 Disabled Accounts

After 30 days of not logging in, user account becomes “Disabled”. User may not log in directly. Browser will be navigated to the USER ID/Password page. User may use “Forgot Password?” link to generate a new password. Previous passwords have expired and cannot be used. Once new password is received, user may re-enable their account from USER ID/Password page.

PDREP-AIS will send daily disabled notifications warning users to re-enable their account until the account is Deactivated.

Users have 15 days from first notification to complete this task.

11.3 Deactivated Accounts

After 45 days of not logging in, user account becomes “Deactivated”. User may not log in. Browser will be navigated to the USER ID/Password page. User may not use “Forgot Password?” link to generate a new password. Previous passwords have expired and cannot be used. User will need to submit a RENEW SAAR-P to regain access.

PDREP-AIS will send a single Deactivation notification informing users the account is Deactivated with instructions to submit a RENEW SAAR-P if access is required.

Users may complete this task as needed.

11.4 End of Contract

For Contractors, accounts are also deactivated on the day of contract expiration as well as Inactivity as noted above. If a contract is extended or a new contract is issued, contractors will need to submit an Access Change Request to update their profiles.

At 7 days before contract end, PDREP will send a single notification reminding contractors to submit Access Change Request.

NOTE: *The Access Change Request needs to be approved by sponsor and processed by PDREP Admin in the 7-day period or it will be rejected because the account will be deactivated and deactivated accounts need to have background investigations re-verified by security managers.*

At contract end, PDREP-AIS will send a single Deactivation notification informing users the account is Deactivated with instructions to submit a RENEW SAAR-P if access is required.

Users may complete this task as needed.

11.5 Deactivation Requests

If users no longer need access to PDREP-AIS, they or their Supervisor/Sponsors may contact the NSLC Portsmouth Help Desk and request that the account be deactivated.

12 ADMINISTRATIVE ACCOUNT ISSUES

12.1 New CAC/PKI Cert

If user receives a new CAC/PIV/CERT and cannot login, contact the NSLC Portsmouth Help Desk to have hash code remove from user profile then resynchronize as outlined in Section 8.1.

12.2 E-Mail Change

User e-mail is a key field and is not available for users to update. If user needs to update their e-mail address, contact the NSLC Portsmouth Help Desk to have information updated in their user profile then resynchronize as outlined in Section 8.1.

12.3 Supervisor Change

If users need to update their supervisors e-mail address, all non DCMA users may go to Edit User Profile link and update the information there (See **Section 10.2**).

DCMA users, due to their unique process, needs to complete an Access Change Request and identifying new supervisors through the Drop Down List.

13 SUMMARY

This concludes the User Access user guide.

Content provided within this document is maintained by the Product Data Reporting and Evaluation Program under the guidance of Naval Sea Logistics Center Portsmouth's Deputy Functional Manager and the Automated Information System Manager.

The User Access user guide is intended to be used as a technical reference document to assist users with system navigation and basic operational functionality within PDREP-AIS. Questions, comments or concerns regarding the User Access module or this guide should be directed to the PDREP Customer Support Desk.

NSLC Portsmouth Help Desk

Contact us by submitting a help desk ticket either via the "Contact Help Desk" button in the lower right

corner of our PDREP website or via the "Help" menu within the PDREP-AIS Application.

Appendix 1 – Notifications

SAAR-P Submittal Notification – USG Employee

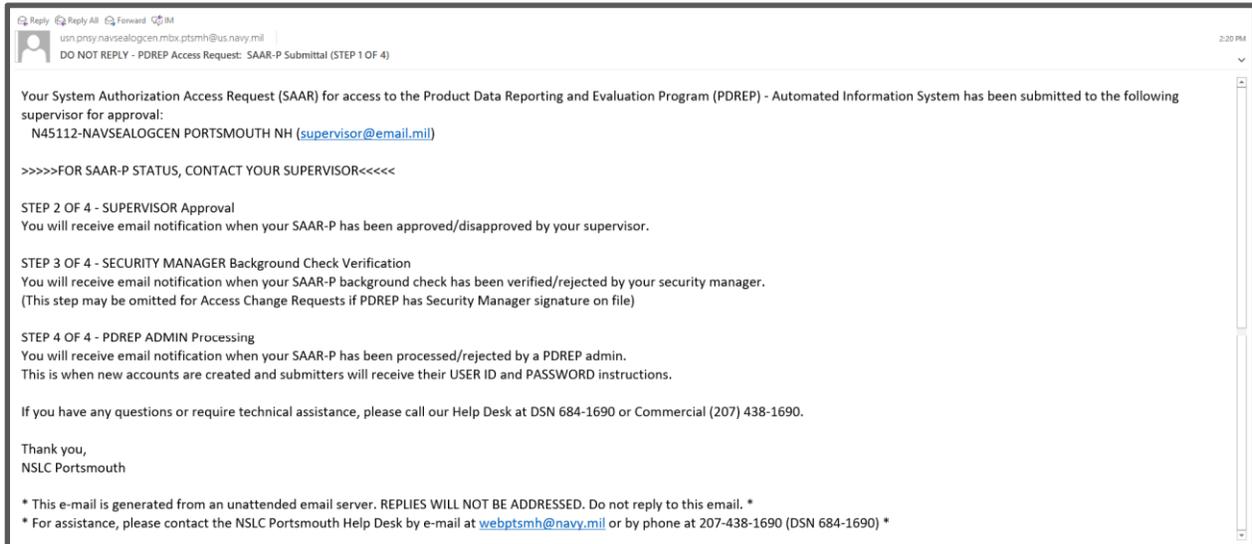


Figure A.1

SAAR-P Submittal Notification – Contractor

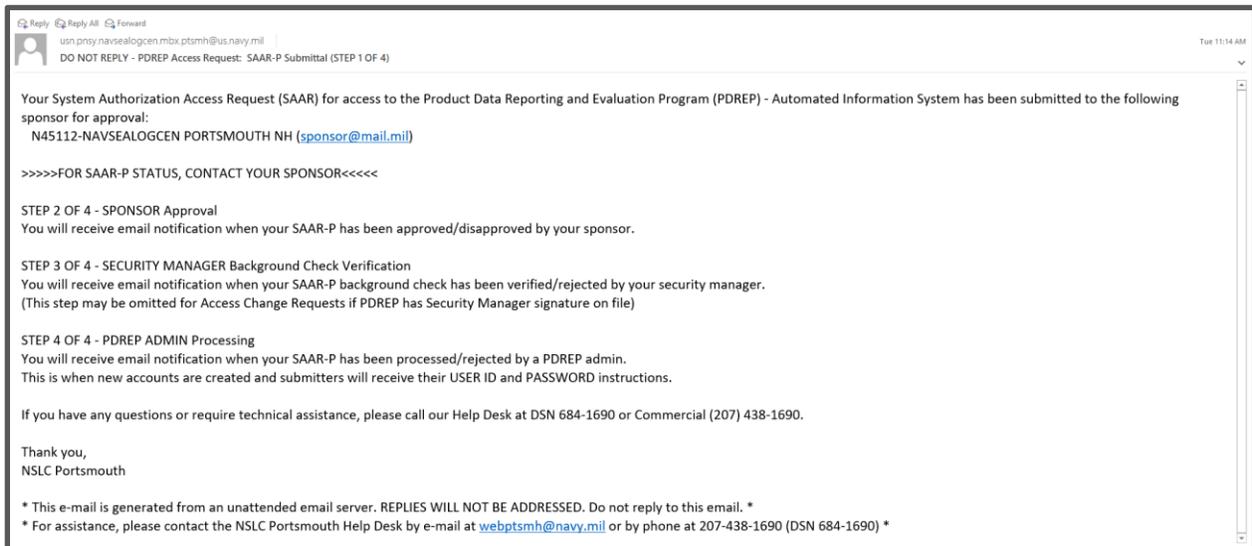


Figure A.2

SAAR-P Supervisor Approval – USG Employee

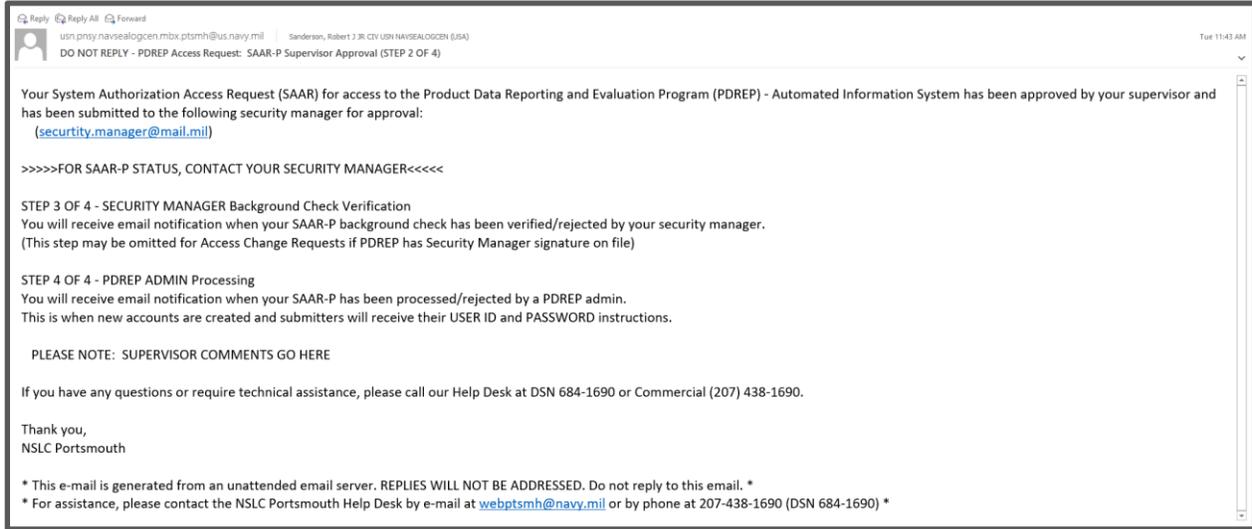


Figure A.3

SAAR-P Sponsor Approval – Contractor

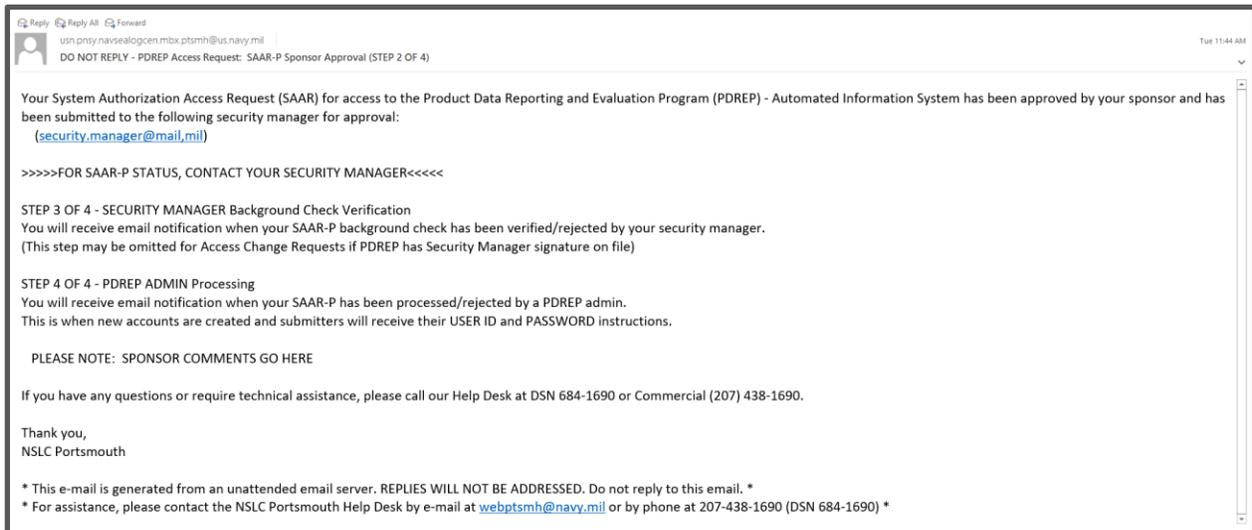


Figure A.4

SAAR-P Supervisor Disapproval – USG Employee

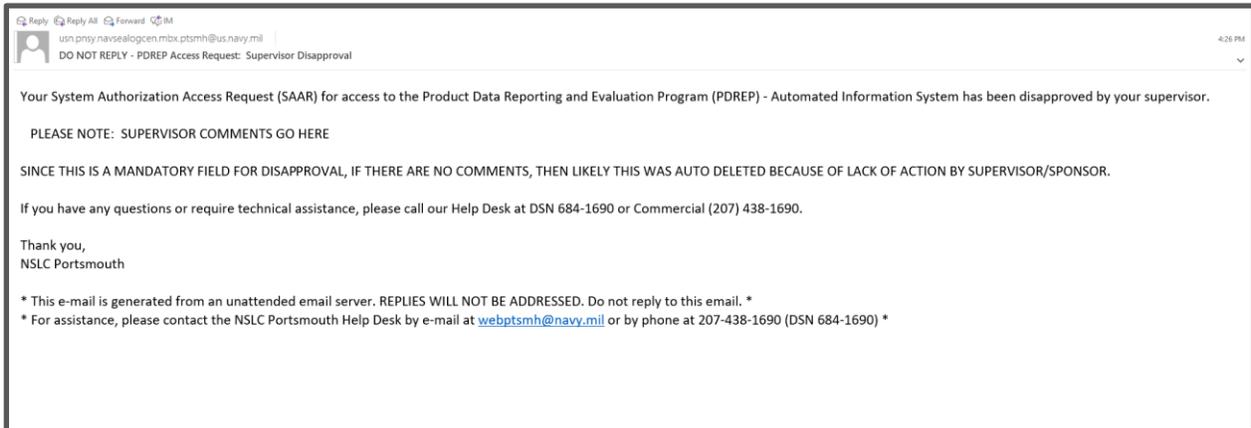


Figure A.5

SAAR-P Sponsor Disapproval – Contractor

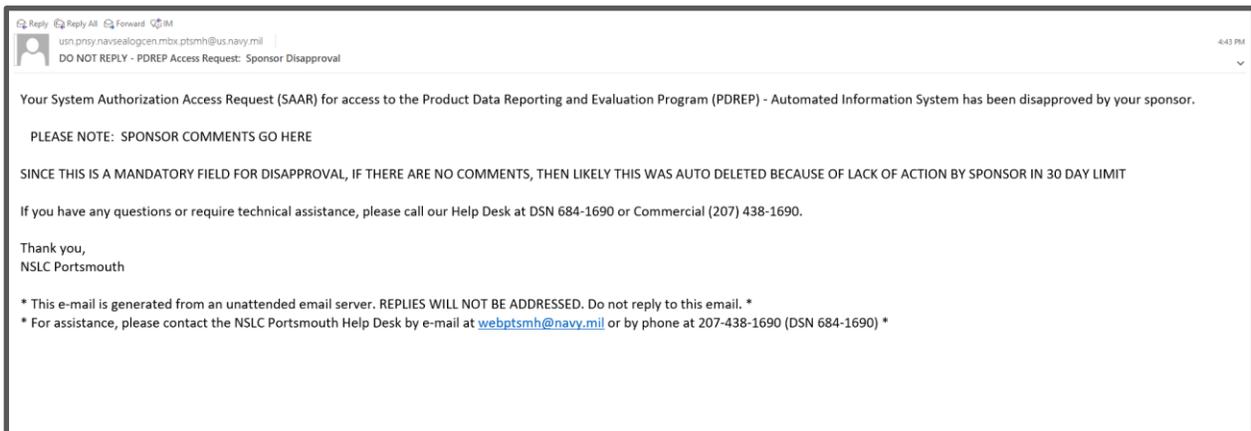


Figure A.6

SAAR-P Security Manager Background Verification

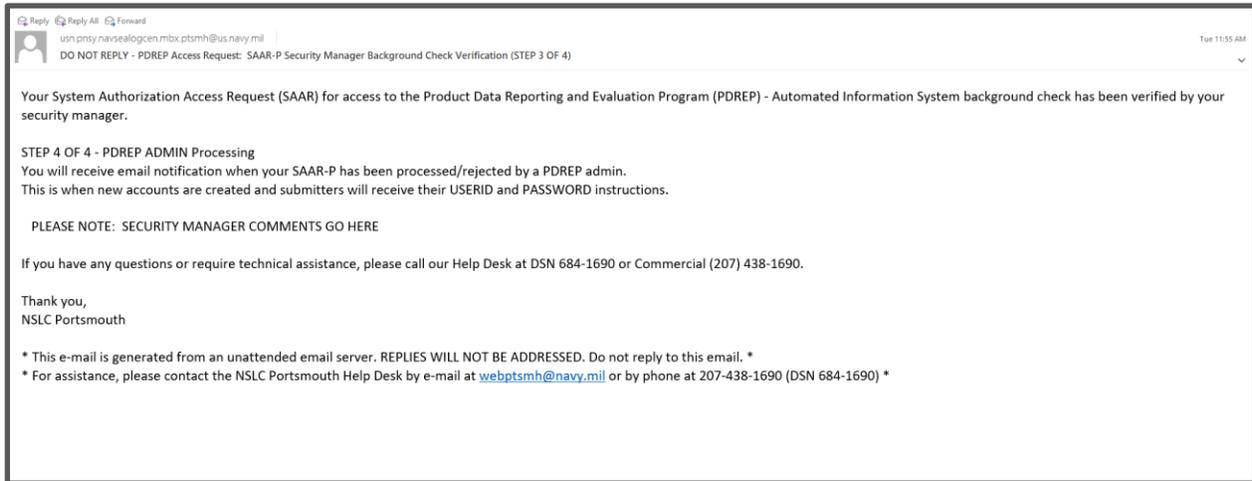


Figure A.7

SAAR-P Security Manager Disapproval

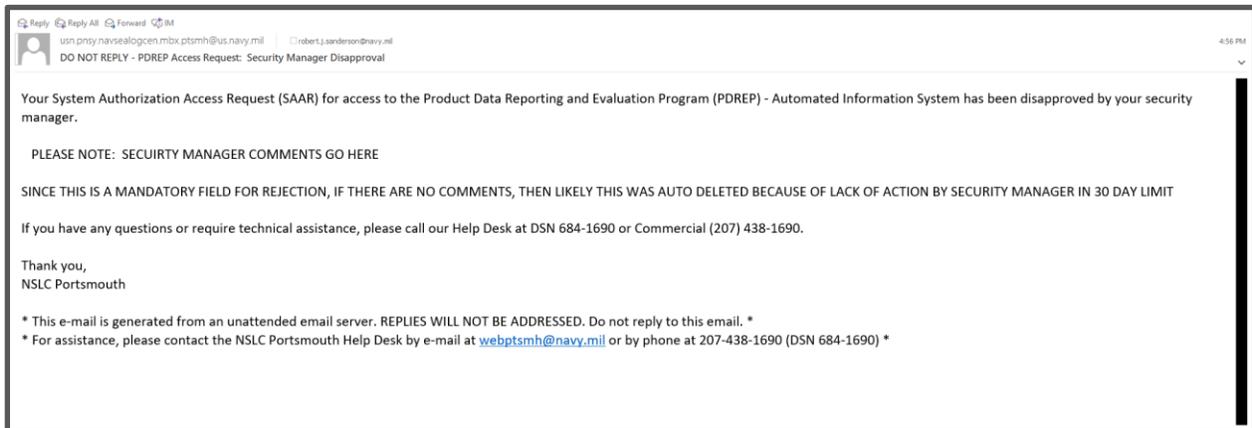


Figure A.8

SAAR-P PDREP Admin Processed

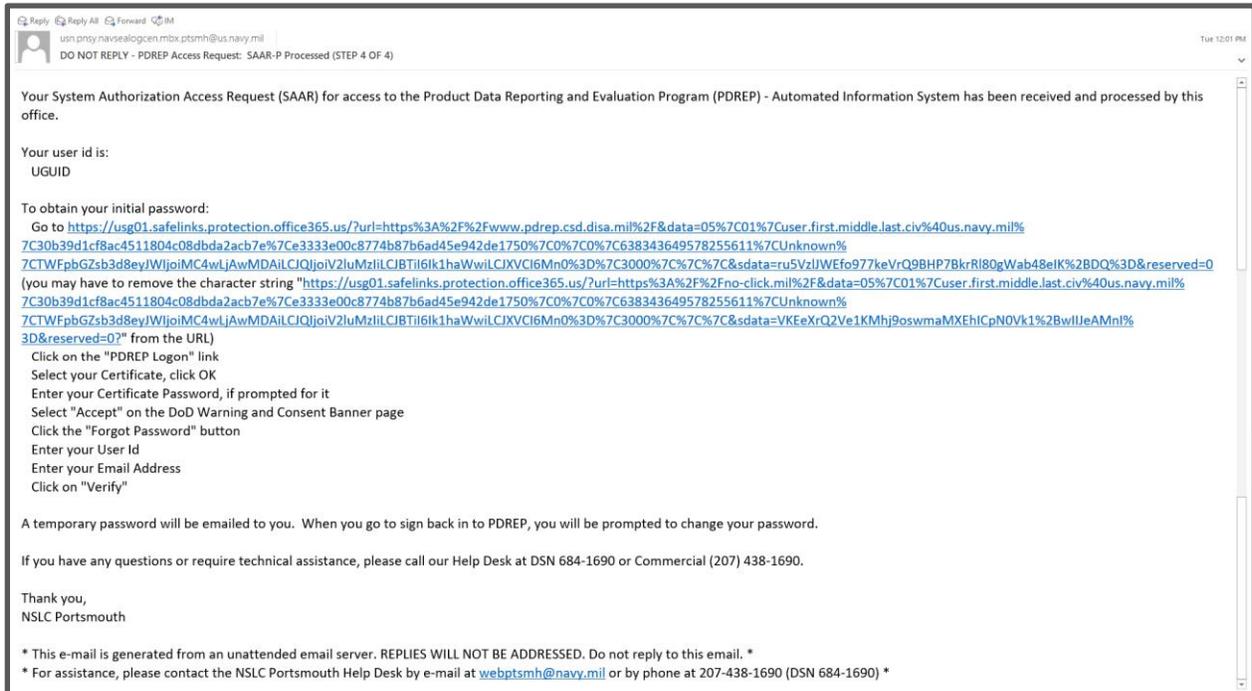


Figure A.9

SAAR-P PDREP Admin Disapproval

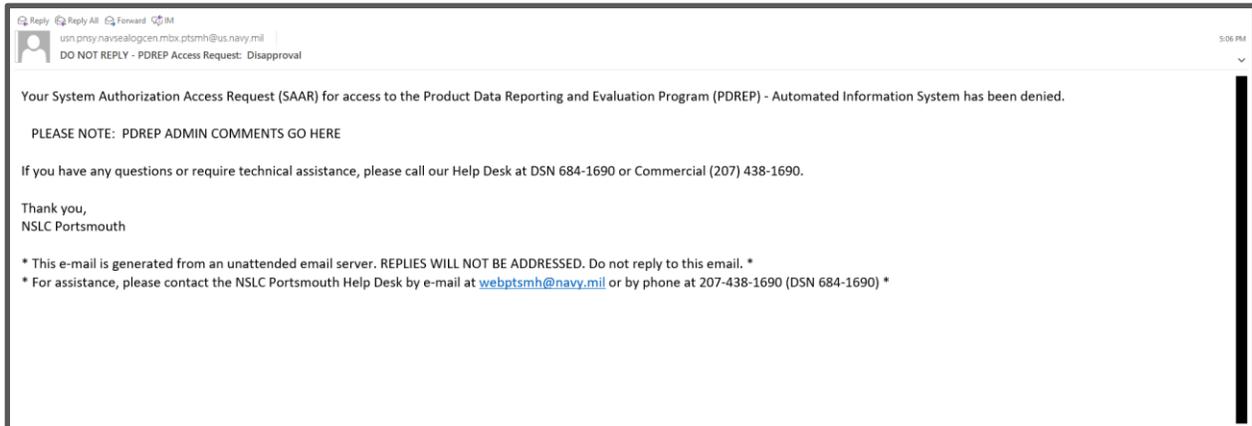


Figure A.10

Security Manager Notification

Reply Reply All Forward IM
usn.pnsy.navsealogcen.mbx.ptsmh@us.navy.mil Sanderson, Robert J JR CIV USN NAVSEALOGCEN (USA) 4:53 PM
DO NOT REPLY - PDREP Access Request: Security Manager Notification

A System Authorization Access Request (SAAR) for access to the Product Data Reporting and Evaluation Program (PDREP) - Automated Information System has been submitted by:
USER ACCESS USER GUIDE (contractor.e-mail@mail.mil)
888-555-1212

Who works for:
N45112-NAVSEALOGCEN PORTSMOUTH NH (supervisor@email.mil)

PLEASE NOTE: SUBMITTER COMMENTS GO HERE

To process the SAAR, please copy and paste the following link to access this request and approve/disapprove (you may have to remove the character string
"<https://usg01.safelinks.protection.office365.us/?url=https%3A%2Fno-click.mil%2F&data=05%7C01%7Cuser.first.middle.last.civ%40us.navy.mil%7C1c024ed72ffc4f19a00308dbdbe5ae83%7Ce3333e00c8774b87b6ad45e942de1750%7C0%7C0%7C638345551746148299%7CUnknown%7CTWFpbGZsb3d8eyJWljoimC4wLjAwMDAilCjQjoiV2luMzliLjBjTl6ik1haWwLjCjXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=KldTkU2PwFv2XORHEycBoM%2BQxwLE55Edmncq%2Ba101Y%3D&reserved=0>" from the URL):
<<https://usg01.safelinks.protection.office365.us/?url=https%3A%2Fcentralpki.csd.disa.mil%2Fpki%2Fcheckcert%3Fappname%3Dpdrepgovt%26loginredirect%3Drequestaccountsecuritymanager%26requestaccountseq%3D10B900512B95E00563A2B97DEF640ED326288&data=05%7C01%7Cuser.first.middle.last.civ%40us.navy.mil%7C1c024ed72ffc4f19a00308dbdbe5ae83%7Ce3333e00c8774b87b6ad45e942de1750%7C0%7C0%7C638345551746148299%7CUnknown%7CTWFpbGZsb3d8eyJWljoimC4wLjAwMDAilCjQjoiV2luMzliLjBjTl6ik1haWwLjCjXVCi6Mn0%3D%7C3000%7C%7C%7C&sdata=%2BHoH6DGaulcdDox5xOohx0tX1FruEVVogOSIV%2BIC88%3D&reserved=0>>

If you have any questions or require technical assistance, please call our Help Desk at DSN 684-1690 or Commercial (207) 438-1690.

Thank you,
NSLC Portsmouth

Figure A.13