Product Data Reporting and Evaluation Program (PDREP)
Automated Information System (AIS)
Access Request Form

Email Completed Access Request Form to: PDREPMail@navy.mil

OR

Fax Access Request Form to : (207) 438-6535

Section A

User Information (To be completed by the user requesting access)

Access Request Type

◯ New ◯ Renew

DoD Data

Last Name: _____ **First:** _____ **MI:** ____

Primary DODAAC: _____ **Additional DODAAC:** _____ **Additional DODAAC:** _____

DoD Activity Name: _____

Office / Activity Code: _____

Office Address: _____

City: _____ **State:** ____ **Zip Code:** _____

Work Phone Number: _____ **Ext:** ____ **DSN:** _____ **Fax:** _____

Government E-Mail Address: _____

Supervisor E-Mail Address: _____

DoD Contractor Data Required

Company Name: _____ **CAGE:** _____

Company Address: _____

City: _____ **State:** ____ **Zip Code:** _____

Phone Number: _____ **Ext:** ____ **Fax:** _____

Company E-Mail Address: _____

Sponsor E-Mail Address: _____

Section B

Access Request (Used to identify the specific functionality required)

PDREP Application Access

Please identify below the Reporting & Retrieval Application functionality required.

☐ **Product Quality Deficiency Report – PQDR Application (Includes Originate PQDRs)**

Please check the block(s) that depict the type of work you do in the PQDR process:

☐ Screening Point ☐ Action Point ☐ Support Point (DCMA ONLY)

◯ QAR (DCMA ONLY) ◯ DRPM (DCMA ONLY)

☐ Master Screener (ARMY ONLY) ☐ Action Officer (ARMY ONLY)

☐ **Supply Discrepancy Report - SDR Application**

☐ Originate SDRs ☐ Action Point

☐ **Ships Critical Safety Item - SCSI (DoD Only)**

◯ Non-Management ◯ CHENG Proxy ◯ TWH Proxy

◯ Management ◯ CHENG ◯ FULL

☐ **Material Inspection Report – MIR**

☐ **Supplier Audit Program – SAP**

☐ **Hull, Mechanical and Electrical (HM&E) Equipment Data Research System – HEDRS**

☐ **Naval Bulletins**

☐ **Level I & Sub-Safe Verification Program**

☐ **Corrective Action Request – CAR**

☐ **Quality Assurance Letter of Inspection / Letter of Delegation - QALI/ LOD**

☐ **Facility Surveillance Inspection Plan - FSIP**

◯ QAR ◯ Team Lead ◯ Contracting Quality Officer

◯ Technical Warrant Holder ◯ NAVSEA 04P ◯ Reviewer

Section C

User Agreement (To be Agreed to and signed by the user requesting access)

USER AGREEMENT - STANDARD MANDATORY NOTICE AND CONSENT PROVISION

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this system) that is provided for U.S. Government-authorized use only.
- You consent to the following conditions:
-- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.
-- At any time, the U.S. Government may inspect and seize data stored on this information system.
-- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purposes.
-- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

- Not withstanding the above, using an information system does not constitute consent to personal misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or service by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
-- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
-- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
-- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
-- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
-- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/ seized privileged communications and data to ensure they are appropriately protected.
- - In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

USER RESPONSIBILTIES

I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- Virus check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents immediately in accordance with local procedures and CJCSM 6510.01 (series).
- Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.
- Be subject to monitoring, and further understand that there is no expectation or right to privacy over the data and communications generated through my use.
- Protect Past Performance Information (PPI) as “SOURCE SELECTION SENSITIVE INFORMATION” in accordance with 41 U.S.C. 423.
- Not attempt to access files for which I do not have access privileges.
- Treat all information examined or extracted pertaining to the companies whose data is in the system as "business sensitive" or "company confidential".
- Not enter or process classified information.
- Properly mark, safeguard and destroy data in accordance with applicable regulations.
- Not transmit or communicate data obtained from the system to any person, contractor, or government employee, who does not have a specific need-to-know.
- Notify NAVSEALOGCEN PORTSMOUTH when I no longer need my account and advise regarding disposition or disposal of database, software packages, and functional accounts.- I will notify NAVSEALOGCEN PORTSMOUTH when I no longer need my account and advise regarding disposition or disposal of database, software packages, and functional accounts.
- Notify NAVSEALOGCEN PORTSMOUTH in case of any security incident.
- Not program function keys or use other capabilities to provide an automatic logon from my device.

I further understand that, when using Navy IT resources, I shall not:

- Auto-forward official e-mail to a commercial e-mail account.
- Bypass, strain, or test Information Assurance (IA) mechanisms (e.g., firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (e.g., Commanding Officer (CO) or Officer in Charge (OIC)).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority.
- Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority.
- Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

User Request Signature and Date

Digital Signature _____ Date _____

Supervisor Signature and Date

As the Supervisor of this user, I certify that this user requires access as requested, has the appropriate level of security clearance, the hardware being used to access the system(s) is accredited, and that I will enforce the above terms and restrictions.

Email to PDREP

Digital Signature _____ Date _____

Section D

Non Government Sponsor Agreement (To be Agreed to and signed by the Government sponsor)

Non-Government Employee - Sponsor Information

Primary Government Point of Contact

Sponsor Name:

Sponsor Activity:

Sponsor Work Phone Number: **Ext:** **DSN:**

Supporting Contract Number: **Expiration Date:**

Government E-Mail Address:

Sponsor Approval Required for all Access Requests for Non-Government Employees

As the US Government Sponsor of this Non Government user, I certify that this user requires access as requested, has the appropriate level of security clearance, the hardware being used to access the system(s) is accredited, and that I will enforce the above terms and restrictions.

Email to PDREP

Digital Signature _____ Date _____