DOD FOCAL POINT ACCESS REQUEST FORM

(NOT FOR REQUESTING ALTERNATE FOCAL POINT ACCESS)

****NOTE: If requesting Alternate Focal Point access, contact you Primary Focal Point.****

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

If using Acrobat 8 or later, this form may be **signed digitally and e-mailed** to NAVSEALOGCEN. Upon completing and digitally signing the form, including the User Agreement, click the button in the signature block to e-mail a digitally signed, completed form to your supervisor or manager for approval, who may then digitally sign and e-mail the approved form to NAVSEALOGCEN for processing.

(See information at the end of this form for alternate *submittal methods if digital signing is unavailable.)*

☐ **REPLACE & DELETE PREVIOUS FOCAL POINT.** *Name and User ID Required

*Previous Focal Point Name:

*Previous Focal Point User ID:

Last Name: **First Name:**

E-mail Address:

Phone: **Ext:** **DSN:** **FAX:**

Office Address:

City/State/Zip:

Service or Agency

☐ DISA ☐ DLA ☐ MDA ☐ SOCOM ☐ TRICARE/TRIMED DoD Other:

Air Force

☐ AFDW	☐ AFICA	☐ AFICA-ACC	☐ AFICA-ACC-AFISRA	☐ AFICA-AETC
☐ AFICA-AFCEC	☐ AFICA-AFGSC	☐ AFICA-AFMSA	☐ AFICA-AFSPC	☐ AFICA-AFSOC
☐ AFICA-AFMOA	☐ AFICA-AMC	☐ AFICA-PACAF	☐ AFICA-USAFE	☐ AFMC
☐ AFOTEC	☐ AFRC	☐ AFTAC	☐ SMC	☐ USAFA
☐ 11th CONS	☐ OTHER			

Navy

☐ CNET	☐ MSC	☐ Marines	☐ NAVAIR	☐ NAVFAC	☐ NAVFLT	
☐ NAVMED	☐ NAVSEA	☐ NAVSUP	☐ ONR	☐ SPAWAR	☐ SSP	☐ OTHER

Army

☐ ACC-APG	☐ ACC-NCR	☐ ACC-PICATINNY
☐ ACC-REDSTONE	☐ ACC-ROCK ISLAND	☐ ACC-WARREN
☐ ACC/ECC/AFRICA	☐ ACC/ECC/EUROPE	☐ ACC/ECC/PARC AMERICAS
☐ ACC/ECC/PARC KOREA	☐ ACC/ECC/PARC PACIFIC	☐ ACC/ECC/PARC SW ASIA
☐ ACC/MICC	☐ ACC/PM SANG	☐ ACC/SDDC
☐ C-JTSCC (AFGHANISTAN)	☐ C-JTSCC (IRAQ)	☐ INSCOM
☐ MEDCOM	☐ MRMC	☐ PEO STRI
☐ SMDC	☐ USACE	☐ OTHER

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 information 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 purpose.
-- 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.
-- Notwithstanding the above, using an information system does not constitute consent to personnel 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 services 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.
-- 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 RESPONSIBILITIES

I agree that I will comply with the terms/restrictions as listed below:

-- Focal Point access is an inherently Government function and is not authorized for support contractor personnel.

-- As a Focal Point I will abide by the policies set in the CPARS Guide when granting access accounts.

-- I understand that Past Performance information is to be protected as "For Official Use Only, Source Selection Information - See FAR 3.104" and I will safeguard data in accordance with regulations.

-- I will not attempt to access files for which I do not have access privileges.

-- I will treat all information examined or extracted as "business sensitive" or "company confidential " data pertaining to the companies whose data is in the system.

-- I will not enter or process classified information.

-- I will not transmit or communicate data obtained from the system to any person, contractor employee or government employee, who does not have a specific need for the information.

-- I will notify NAVSEALOGCEN PTSMH when I no longer need my account and advise regarding disposition or disposal of database, software packages, and functional accounts.

-- I will notify NAVSEALOGCEN PTSMH in case of any security incident.

-- I will not program function keys or use other capabilities to provide an automatic logon from my device.

Focal Point Signature
Focal Point must be a government employee, not contractor support personnel.
This signature acknowledges your consent to and agreement with previously stated User Agreements and Responsibilities.

⇨⇨⇨**THIS FORM WILL NOT BE APPROVED WITHOUT NAME, DATE and SIGNATURE**⇦⇦⇦

Print Name (Focal Point) **Date**

Focal Point Digital Signature:

Submit for Approval*

Print Form

(Click in field to digitally sign and lock field entries. Right click to clear signature and unlock fields to enable revising entries.)

***Air Force & Army require MAJCOM/MACOM signature in place of Supervisor.**

When prompted after applying digital signature, "Save" the digitally signed, completed form. Click the button to the right of the signature block to e-mail it to the manager or supervisor (or MAJCOM/MACOM if Air Force or Army) whose address you enter in the "To:" block of the e-mail.

Focal Point Supervisor Signature*
***Air Force & Army requires MAJCOM/MACOM signature in place of Supervisor.**
(Contact CPARS Help Desk for specific contacts.)

⇨⇨⇨**THIS FORM WILL NOT BE PROCESSED WITHOUT NAME, DATE and SIGNATURE**⇦⇦⇦

Print Name (Authorizing Official) **Date**

Authorizing Official Digital Signature:

Submit to NAVSEALOGCEN

Print Form

(Click in field to digitally sign and lock field entries. Right click to clear signature and unlock fields to enable revising entries.)

When prompted after applying digital signature, "Save" the digitally signed, digitally approved, completed form. Click the button to the right of the signature block to e-mail it to NAVSEALOGCEN.

Signing and Sending Instructions

If using Acrobat 8 or later, this form may be **signed digitally and e-mailed** to NAVSEALOGCEN.
Upon completing and digitally signing the form, including the User Agreement, click the button in the signature block to e-mail a digitally signed, completed form to your supervisor or manager for approval, who may then digitally sign and e-mail the approved form to NAVSEALOGCEN for processing.

If digital signing is not available:

Fax completed and signed forms to:

207-438-6535

or

Postal mail completed and signed form to:

Naval Sea Logistics Center Portsmouth
Bldg. 153-2, Portsmouth Naval Shipyard,
Portsmouth, NH 03804-5000

For NAVSEALOGCEN PTSMH Use Only

User ID:

Date:

Approval Authority: