# HPCMP User Agreement

Welcome to the DoD High Performance Computing Modernization Program (HPCMP). By agreeing to the contents of 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 are consenting to the following conditions:

## Requirements

- DoD HPC Centers' resources shall be used ONLY for official Government business. Copyrighted or proprietary software shall not be executed, copied from, or stored on these systems without proper authorization.

- I hereby acknowledge that I am completely responsible for my User Accounts (usernames and accounts issued by the HPC Centers) and will protect them as "For Official Use Only" (FOUO) or, where applicable, CLASSIFIED at the appropriate level. I UNDERSTAND THAT USER ACCOUNTS WILL NOT BE SHARED WITH ANYONE FOR ANY REASON AT ANY TIME. I will report use of said User Account by other persons of which I become aware to the Consolidated Customer Assistance Center (CCAC). I understand that the HPCMP Information Systems Security Officer (ISSO) or designee will investigate all security, unauthorized access, and abuse incidents. I understand user activities are audited and that misuse of any HPC Centers resources may result in disciplinary action and/or denial of computing privileges.

- Upon leaving the DoD HPCMP, I will notify my S/AAA to close my accounts.

- I hereby agree to obtain prior permission to access any HPCMP resources from any location outside of the United States, by completing the International Access Authorization Request in the Portal to the Information Environment (pIE) . I will not access any HPCMP resources from any location outside of the United States until the HPC Modernization Program Office approves my request.

- I hereby state the work I am doing is in support of a United States DoD project, including The Technical Cooperation Program (TTCP) Group (Australia, Canada, New Zealand, United Kingdom of Great Britain and the United States; I hold the appropriate country clearance). I will not utilize the DoD HPCMP resources on behalf of any foreign government with the exception of the above four listed countries for TTCP matters.

- It is agreed that any publications resulting from research supported by this HPC grant will include the following credit statement: "This work was supported in part by a grant of computer time from the DoD High Performance Computing Modernization Program at (fill in HPC Center's name(s))".

- Open research system users are not permitted to introduce, process, or store sensitive data on any open research systems. Users of open research systems who do not have a NACI will be required to provide proof of citizenship (and current visa, if applicable) and to consent to routine background checks.

- Project Leaders agree that software (source code and documentation) developed in this project and having potential for DoD re-use will be made available where appropriate.

**Security Information**

- 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.

- 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.

.

☐ I agree

**Date:** _____ **Full Name:** _____

**Signature:** _____

==========

created 04/03/2013

revised 6/10/2013

***Rule: If the user does not agree, user message pops up that the account process has been terminated until user agrees to terms and conditions in this document.***