

INFORMATION SYSTEM USER AGREEMENT

This user agreement is to be used in conjunction with DD Form 2875 system access request form.

USER AGREEMENT

This document details some of the duties and requirements established by existing law, executive orders, regulations, and instructions for the use of Department of Defense (DoD) Information Systems (IS).

1. The Non-classified Internet Protocol Router Network (NIPRNet) users have the responsibility to safeguard the information contained in the systems from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. The NIPRNet is for official use and authorized purposes in accordance with DoD 5500.7-R, "Joint Ethics Regulation." Information on the system is subject to monitoring and security testing.
2. NIPRNet is the primary unclassified automated administration tool for the Defense Acquisition University (DAU).
 - a. NIPRNet provides unclassified communication to external DoD and other U.S. Government (USG) organizations via electronic mail and network protocols from NIPRNet.
 - b. NIPRNet is approved to process UNCLASSIFIED information in accordance with DoD and DAU policies.
 - c. The NIPRNet and the Internet, as viewed by the DAU are synonymous. Minimal security exists on this system. E-mail and attachments are vulnerable to interception as they traverse the NIPRNet and the Internet.
3. As a NIPRNet system user, the following security rules and requirements apply:
 - a. Personnel are not permitted access to the NIPRNet unless they are in compliance with the DAU personnel security requirements for operating on these systems.
 - b. The currently approved DAU Information Assurance training program is required for all military, civilian, and contractor personnel before receiving system access.
 - c. Passwords must be safeguarded. Personal password sharing and embedded passwords is prohibited.
 - d. Secure passwords will consist of at least 15 characters and random combinations of uppercase and lowercase letters, numbers, and special characters. Do not use your user ID, common names, birthdays, phone numbers, or dictionary words.
 - e. Only USG-acquired hardware and software are authorized. Use of any personally owned hardware, software, shareware, or public domain software without the expressed permission or approval of the DAU DAA is prohibited.
 - f. Virus-checking is mandatory prior to uploading information onto any DAU system via the NIPRNet or removable media (flash drives, CDs, etc).
 - g. Users will not attempt to access or process data or use operating systems or programs, except as specifically authorized. Users will not upload .exe, .com, .vbs or .bat files onto either system without DAA permission. Users will not introduce malicious code to USG IS.
 - h. Users will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated on office automation networks (i.e., printed output, magnetic tapes, floppy disks, and downloaded hard-disk files) whether in the form of messages, electronic mail, word processing documents, spreadsheets, databases, graphical presentations, or are IAW EO 12958, "Classified National Security Information," and DoD 5200.1-R, "Information System Security Program."
 - i. No maintenance will be performed on any workstation without authorization from a system administrator.
 - j. Log-off or screen-lock the workstation when leaving the area. Log-off the workstation at the end of each working day.
 - k. Users can notify a system administrator and/or information assurance officer with any questions regarding policy, responsibilities, and duties. Do not hesitate. Report all security incidents immediately.
- l. By signing this user agreement, you confirm that you have read, understand and agree with this agreement as well as DAU Directives 303 and 304.
- m. Failure to comply with the above requirements may result in a) revoking of NIPRNet access, b) counseling, c) criminal prosecution, d) discharge or loss of employment and e) revocation of security clearance.

NOTICE AND CONSENT STATEMENT

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.
 - 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.

1. NAME (*Last, First, Middle Initial*)

2. USER SIGNATURE

3. DATE (*YYYYMMDD*)