

FRCWESTPAC INFORMATION ASSURANCE (IA) USER AWARENESS AGREEMENT (UAA)

1. Every person who uses or manages DoD information systems (military, government civilian, contractor) has a responsible security role. All users have a personal responsibility to protect information processed on NAVAIR information systems. Key roles and responsibilities are outlined in Appendix A to Enclosure A of the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 of 25 Mar 2003, "IA and Computer Network Defense (CND)." This manual requires that users sign a UAA prior to being granted system access. It is also a requirement that the UAA be reviewed periodically to ensure it meets current requirements and regulations. This revision, dated 27 July 2004 meets the most current requirements. Information Assurance (IA) is not merely a bureaucratic requirement. Unsafe practices by our users make Navy networks vulnerable to threats like bandwidth saturation, social engineering, phishing and imbedded malware. All of these threats can be averted if our people understand their IA obligations and the significant cost of noncompliance
2. By my signature, I certify that I have read and agree to the following terms. Failure to do so can result in denial of access to DoD information systems. If I have questions relative to IA at any time during my employment, it is my responsibility to contact the FRCWESTPAC IA Manager Program Office (IAM) via my appointed Information Assurance Officer (IAO). The terms of this agreement apply to all DoD information systems and Information Technology (IT) resources that I access.
3. I will follow the check-in process and the check-out process in accordance with FRCWESTPAC policy. When my need or authorization for accessing any information system or network terminates, and especially at job termination, I will notify the affected IAOs, System Administrators (SAs) and other appropriate authorities so system access permissions can be terminated and I will not attempt further access.
4. I will attend all required training, both prior to initial system access and annually, that is made available to me.
5. I will not discuss or transmit classified information over non-secure circuits. I understand that official DoD telecommunications systems and automated information systems are subject to COMSEC monitoring at all times and that use of these systems constitutes consent to being monitored. I understand that the following legally approved logon-warning banner must be displayed on all government computer systems. I understand that the use of any computer system processing government data constitutes consent to monitoring. My signature at the end of this UAA constitutes my explicit consent to being monitored.
6. I will use DoD information systems only for official use and authorized purposes in accordance with DoD 5500.7-R, "Joint Ethics Regulation," paragraph 2-301, Use of Federal Government Resources, and DoD Instruction O-8530.2, "Support to CND." I will contact my IAO for clarification if I am uncertain as to whether my use constitutes official and authorized purposes.
7. I will only access data or use operating systems or application programs as authorized. I will not duplicate copyrighted software without the express written permission of the author/distributor and will only use software on the computer systems for which they are intended. I understand I may be held personally accountable for software copyright violations I commit.
8. I will not load or use entertainment software, shareware or public domain software on any DoD information system without express written permission from the NAVAIR Designated Approving Authority (DAA). I will not attempt to access or process data or use operating systems or programs, except as specifically authorized by the DAA. I will not upload .exe, .com, .vbs, or .bat files onto any system without DAA permission and I will not write malicious code.
9. I will not bring personally owned information processing resources (e.g. Palm Pilots, laptops, two-way pagers, cell phones, digital cameras, etc.) into areas where classified data can be processed. All IT devices that transmit Radio Frequency (RF) signals are PROHIBITED from areas where classified data can be processed. Personally owned IT devices cannot be connected to DoD information systems.
10. I will protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.

Prior to disclosing or releasing any DoD-related data, I will ensure the appropriate need-to-know approvals are in place and/or that the information has been cleared for public release. I will log-off or screen-lock my workstation prior to leaving it unattended. I will log-off the workstation at the end of each working day. I will ensure classified and CUI is appropriately marked, handled, and stored IAW DoD and FRCWESTPAC guidelines. I have read and agree to abide by the security SOPs for each information system to which I am granted access. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated on DoD systems and networks (e.g., printed output, magnetic tapes, floppy disks, CDs, and downloaded files) whether in the form of messages, electronic mail, word processing documents, spreadsheets, databases, graphical presentations, etc., in accordance with Executive Order 12958, "Classified National Security Information," and DoD 5200.1-R.

11. My password(s) shall be a minimum of fourteen characters in length for unclassified systems for which I'm authorized access, and they will contain alpha, numeric, and special characters. I understand passwords should not be constructed from personal data, e.g., social security number, telephone numbers, relative's names, etc. My passwords will be 14 characters in length for the classified systems for which I'm granted access. I will not process classified information on any information system not specifically approved for this purpose and will report any inadvertent or unapproved classified processing to the IAM via the IAO immediately so that the system can be sanitized. I will protect passwords and remote access telephone numbers from unauthorized access and will not share them with coworkers or other individuals. I will not allow anyone to use my account, e.g., UserID and password, to gain access to a system/network for which they have not been given their own UserID and password. I will change my passwords at least every 90 days or as required by system operating procedures. I will not attempt to access systems or accounts for which I have not been granted official, authorized access. I understand that embedded passwords are prohibited and that the SA may employ password tools to identify weak or non-complaint passwords.

12. I will immediately report to the FRCWESTPAC IAM via my appointed IAO any suspected or confirmed computer-related incident of intrusion, malicious code, unauthorized or inappropriate use and/or compromise of any DoD information system. I will report all loss, theft, or damage to computer systems and I will not remove information processing systems or DoD data from FRCWESTPAC facilities unless I have express written permission.

13. I will not transmit DoD information to non-DoD entities (e.g., foreign representatives, contractors, etc.,) from DoD information systems without ensuring the appropriate approvals are in place. Refer to DoD Directive 5230.20 and CJCSI 6211.02B for more details.

14. I understand that virus checking is mandatory prior to uploading information onto any system via any media (e.g., CDs, disks) or electronic connection (e.g., NIPRNet, SIPRNet, etc.,). I will ensure that anti-viral software is loaded on my system/network and that all files, documents and e-mails are scanned before distribution.

15. I will ensure that no maintenance will be performed on any information resource I access without proper authorization from the IAO or SA. I will report all information system or network problems to the SA and/or IAO.

16. I Understand that as a user of FRCWESTPAC network resources I will not bypass or attempt to bypass security controls, by use of an anonymous web proxy, established security mechanisms in order to gain access to unauthorized web sites and web functionality such as web mail, video streaming, music streaming, movies streaming, file sharing, blogging, chat, etc.. This behavior puts Navy networks at risk and degrades network capability, resulting in latency and denial of service.

17. I have read the above requirements regarding the use of DoD information systems. I understand my responsibilities regarding my access to these systems. I understand that violation of any of these rules may be grounds for denial of system use and/or management action or criminal prosecution. This does not relieve me from complying with other regulations as given in various documents, including the Computer Security Act of 1987 (P.L. 100-235), DoDD 8500.1, DoDI 8500.2, NAVAIRINST 5239 (series) and FRCWESTPACINST 5239.2D.

**STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS**

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

(a) 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.

(b) You consent to the following conditions:

(1) 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.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) 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.

(4) 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.

(5) 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:

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(c) 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, (Le., 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.

(d) 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.

<u>Last Name, First, MI</u>	<u>Code</u>	<u>Signature/Phone Number</u>	<u>Date</u>
-----------------------------	-------------	-------------------------------	-------------

** Please forward the signed original FRCWESTPAC IA UAA to the FRCWESTPAC IAM, where it will be maintained on file. **