NAVAL AIR SYSTEMS COMMAND (NAVAIR)
INFORMATION ASSURANCE USER AWARENESS AGREEMENT

1. 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 NAVAIR computer systems and networks. If I have questions relative to computer and telecommunications security at any time during my employment, it is my responsibility to contact the Naval Air Systems Command Headquarters (NAVAIRHQ), Patuxent River, AIR-7.4.2, Information Systems Security Manager (ISSM), via my Information Systems Security Officer (ISSO) or Competency Point of Contact (POC). The terms of this apply to "all" government computer systems/networks that I have access to.

2. I will not process classified information on any computer system not specifically approved for this purpose and will report any inadvertent/unapproved classified processing to the ISSM via the ISSO or Competency POC immediately so that the system can be sanitized.

3. 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.

4. I will protect magnetic media and store them per requirements for the most sensitive data stored and processed following NAVAIR, Navy and Department of Defense (DoD) policies.

5. I will protect passwords and dial-up telephone numbers from unauthorized access and will not share them with coworkers or other persons. I will change my passwords at least every six months or as required by System Operating Procedures (SOPs).

6. I will not remove computer systems or government data from government workspaces without express written permission.

7. I will report all loss, theft, or damage to computer systems.

8. I will not bring personally owned information processing resources into U.S. Government work spaces without written approval.

9. I will not load or use entertainment software on any U.S. Government computer system/network residing in U.S. Government workspaces without express written permission.

10. I will use U.S. Government computer systems only for official use and authorized purposes following the Joint Ethics Regulation (JER), DoD Directive 5500.7-R, paragraph 2-301, Use of Federal Government Resources.

11. I will promptly report to NAVAIRHQ, Patuxent River, AIR-7.4.2, ISSM via the ISSO/Competency POC any suspected or confirmed incident of intrusion, malicious code and/or compromise of any U.S. Government computer system.

12. I have read and agree to abide by the security SOPs for each computer system or network to which I am granted access.

13. I will not attempt access to systems or accounts to which I have not been granted access.

14. I understand that a 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 is my explicit consent to being monitored. I have read and agree with the attached

15. When my need or authorization for accessing any computer system or network terminates, and especially at job termination, I will notify the affected ISSOs or other appropriate authorities so system access permissions can be terminated and I will not attempt further access.

16. 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 laws and regulations, including but not limited to, the Computer Security Act of 1987 (P.L. 100-235), OPNAVINST 5239.1, and NAVAIRINST 5239.2.

Print Name	Competency Code	Sign Name	Date

** Please forward this signed original Information Assurance User Awareness Agreement to be held on file by NAVAIR 7.4.2.

APPROVED DOD WARNING BANNER

* Discussion/transmission of classified information over non-secure circuits is prohibited. Official DoD telecommunications systems and automated information systems are subject to COMSEC monitoring at all times and use of these systems constitutes consent to being monitored.

* ALCOM SUBJ: COMSEC AND INFORMATION SYSTEMS MONITORING REQUIREMENTS
DTG: 131256Z MAY 97, provides policy and guidance on COMSEC and information systems monitoring restrictions. It is DoD and Navy Policy that the following warning banner be displayed on all DoD automated information systems.

"THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."