SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of Individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records will be maintained in paper form.

ROUTINE USES: None.

DISCLOSURE : Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST

□ initial □ Modification □ DEACTIVATE □ USER ID ____________________

DATE (YYYYMMDD)

SYSTEM NAME *(i.e., NMCI, IT21, OneNET, etc.)*

LOCATION *(Physical Location of System)*

PART I *(To be completed by Requester)*

1. NAME (Last, First, Middle Initial)

2. SOCIAL SECURITY NUMBER (LAST FOUR)

3. ORGANIZATION

4. OFFICE SYMBOL/DEPARTMENT

5. PHONE *(DSN and Commercial)*
DSN: COM:

6. OFFICIAL E-MAIL ADDRESS

7. JOB TITLE AND GRADE/RANK

8. OFFICIAL MAILING ADDRESS

9. CITIZENSHIP
□ US □ FN
□ Other

10. DESIGNATION OF PERSON
□ Military □ Contractor
□ Civilian

11. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

□ I have completed Annual Information Awareness Training. DATE (YYYYMMDD) ______________________

12. USER SIGNATURE

13. DATE (YYYYMMDD)

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 17a).*

14. JUSTIFICATION FOR ACCESS

15. TYPE OF ACCESS REQUIRED:
□ AUTHORIZED □ PRIVILEGED

16. USER REQUIRES ACCESS TO:
□ UNCLASSIFIED □ CLASSIFIED (Specify Category): ______________________ □ OTHER: ______________________

17. VERIFICATION OF NEED TO KNOW

I certify that this user requires access as requested. □

17a. ACCESS EXPIRATION DATE (*Contractors must specify Company Name, Contract Number, Expiration Date.*

18. SUPERVISOR'S NAME *(Print Name)*

18a. SUPERVISOR'S SIGNATURE

18b. DATE (YYYYMMDD)

19. SUPERVISOR'S ORGANIZATION/DEPARTMENT

19a. SUPERVISOR'S E-MAIL ADDRESS

19b. PHONE NUMBER

20. SIGNATURE OF INFORMATION OWNER/OPR

20a. PHONE NUMBER

20b. DATE (YYYYMMDD)

21. SIGNATURE OF IAO OR APPOINTEE

22. ORGANIZATION/DEPARTMENT

23. PHONE NUMBER

24. DATE (YYYYMMDD)

25. NAME (*Last, First, Middle Initial)*	25a. SOCIAL SECURITY NUMBER (LAST FOUR)

26. 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.
  - 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.

27. USER SIGNATURE	28. DATE (YYYYMMDD)

29. NAME (*Last, First, Middle Initial)*	29a. SOCIAL SECURITY NUMBER (LAST FOUR)

30. USER RESPONSIBILITIES

I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- Virus check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents immediately in accordance with local procedures and CJCSM 6510.01 (series).
- Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.

I further understand that, when using Navy IT resources, I shall not:

- Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO!, AOL, etc.)
- Auto-forward official e-mail to a commercial e-mail account.
- Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (CO or OIC).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority.
- Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority.
- Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority.
- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

31. USER SIGNATURE	32. DATE

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

33. TYPE OF INVESTIGATION	33a. DATE OF INVESTIGATION (YYYYMMDD)
33b. CLEARANCE LEVEL	33c. IT LEVEL DESIGNATION □ LEVEL 1 □ LEVEL 2 □ LEVEL 3

34. VERIFIED BY *(Print name)*	35. SECURITY MANAGER TELEPHONE NUMBER	36. SECURITY MANAGER SIGNATURE	37. DATE (YYYYMMDD)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

38. TITLE:	38a. SYSTEM	38b. ACCOUNT CODE
	38c. DOMAIN	
	38d. SERVER	
	38e. APPLICATION	
	38f. DIRECTORIES	
	38g. FILES	
	38h. DATASETS	
39. DATE PROCESSED (YYYYMMDD)	39b. PROCESSED BY (*Print name and sign)*	39c. DATE (YYYYMMDD)
40. DATE REVALIDATED (YYYYMMDD)	40a. REVALIDATED (*Print name and sign)*	40b. DATE (YYYYMMDD)

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing
or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.
(2) Social Security Number. The last four numbers in the social security number of the user.
(3) Organization. The user's current organization (i.e., USS xx, DoD, and government agency or commercial firm).
(4) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
(5) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
(6) Official E-mail Address. The user's official e-mail address.
(7) Job Title/Grade/Rank. The civilian job title (i.e., Systems Analyst, YA-02, military rank (CAPT, United States Navy) or "CONT" if user is a contractor.
(8) Official Mailing Address. The user's official mailing address.
(9) Citizenship (U.S., Foreign National or Other).
(10) Designation of Person (Military, Civilian, Contractor).
(11) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
(12) User's Signature. User must sign the OPNAV 5239/14 with the understanding that they are responsible and accountable for their password and access to the system(s).
(13) Date. The date the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(14) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
(15) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters or settings.)
(16) User Requires Access To. Place an "X" in the appropriate box. Specify category.
(17) Verification of Need to Know. To verify that the user requires access as requested.
(17a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
(18) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
(18a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
(18b) Date. Date supervisor signs the form.
(19) Supervisor's Organization/Department. Supervisor's organization and department.
(19a) E-mail Address. Supervisor's e-mail address.
(19b) Phone Number. Supervisor's telephone number.
(20) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
(20a) Phone Number. Functional appointee telephone number.
(20b) Date. The date the functional appointee signs the OPNAV 5239/14.
(21) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to
the system being requested.
(22) Organization/Department. IAO's organization and department.
(23) Phone Number. IAO's telephone number.
(24) Date.The date IAO signs the OPNAV 5239/14.
(25) Name. The last name, first name, and middle initial of the user.
(25a) Social Security Number. The last four numbers in the user's social security number.
(26) Standard Mandatory Notice and Consent Provision. This item is in accordance with DoD memo dtd May 9, 2008 (Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement.
(27) User Signature. User signs.
(28) Date. Date signed.
(29) Name. The last name, first, name and middle initial of the user.
(29a) Social Security Number. The last four numbers in the social security number of the user.
(30) User Responsibilities
(31) User Signature. Member signs.
(32) Date. Date signed.

C. PART III: Certification of Background Investigation or Clearance.

(33) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI or SSBI).
(33a) Date of Investigation. Date of last investigation.
(33b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(33c) IT Level Designation. The user's IT designation (Level I, Level II or Level III).
(34) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(35) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
(36) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
(37) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the functional activity or the customer with approval from NAVNETWARCOM. This information will specifically identify the access required by the user.
(38 - 40b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If transmitted electronically, the email must be digitally signed and encrypted.

FILING: Retention of this form shall be in accordance with SECNAV M5210-1, Records Management Manual (Section 5230.2 applies).