SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM0500-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
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: INPUT DOD ID #

DATE (DDMMMYYYY):

SYSTEM NAME (Platform or Application):
ONE-NET

LOCATION (Physical Location of System):
BAHRAIN / COMUSNAVCENT

PART I (To be completed by Requester)

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

2. ORGANIZATION:

3. OFFICE SYMBOL/DEPARTMENT:

4. PHONE (DSN and Commercial):
DSN: 439-
COMM: 011-973-1785-

5. OFFICIAL E-MAIL ADDRESS:

6. JOB TITLE AND GRADE/RANK:

7. OFFICIAL MAILING ADDRESS:

8. CITIZENSHIP:

____US ____FN

____LN ____Other:________________

9. DESIGNATION OF PERSON:

____MILITARY ____CIVILIAN

____CONTRACTOR

10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS (Complete as required for user or functional level access.):

____I have completed Annual IA Awareness Training. DATE (DDMMMYYYY):__________________________

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 14a).

11. JUSTIFICATION FOR ACCESS:
IN ORDER TO PERFORM DUTIES AND RESPONSIBILITIES.
Derivative Classification Training Completed on:DD/MMM/YYYY

12. TYPE OF ACCESS REQUIRED:
☑ AUTHORIZED □ PRIVILEGED

12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form.

DATE SIGNED (DDMMMYYYY):
____

13. USER REQUIRES ACCESS TO:
☑ UNCLASSIFIED ☑ CLASSIFIED (Specify Category): SIPR □ OTHER:__________________

14. VERIFICATION OF NEED TO KNOW:

I certify that this user requires access as requested. ☑

14a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date):

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT:

15a. SUPERVISOR'S E-MAIL ADDRESS:

15b. PHONE NUMBER:

16. SUPERVISOR'S NAME (Print Name):

16a. SUPERVISOR'S SIGNATURE:

16b. DATE (DDMMMYYYY):

17. SIGNATURE OF INFORMATION OWNER/OPR:

17a. PHONE NUMBER:

17b. DATE (DDMMMYYYY):

18. SIGNATURE OF IAM OR APPOINTEE:

19. ORGANIZATION/DEPARTMENT:

20. PHONE NUMBER:

21. DATE (DDMMMYYYY):

22. 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.

USER RESPONSIBILITIES:

I understand that to ensure the confidentiality, integrity, availability, and security of Navy Information Technology (IT) resources and information, when using those resources, I shall:
- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV), National Security Systems (NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Virus-check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.
- Digitally sign and encrypt e-mail in accordance with current policies.
- Employ sound operations security measures in accordance with DOD, DON, service and command directives.

(Block 22 Cont)

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

- Auto-forward any e-mail from a Navy account to commercial e-mail account (e.g, .com).
- Bypass, stress, or test IA or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).
- 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 the Local IA Authority (i.e., person responsible for the overall implementation of IA at the command level).
- Use personally owned hardware, software, shareware, or public domain software without written authorization from the Local IA Authority.
- Upload/download executable files (e.g., exe, .com, .vbs, or .bat) onto Navy IT resources without the written 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.
- Use Navy IT resources in a way that would reflect adversely on the Navy. Such uses include 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 PII, and other uses that are incompatible with public service.
- Place data onto Navy IT resources possessing insufficient security controls to protect that data at the required classification (e.g., Secret onto Unclassified).

23. NAME (Last, First, Middle Initial):	24. USER SIGNATURE:	25. DATE SIGNED (DDMMMYYYY):

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

26. TYPE OF INVESTIGATION:	26a. DATE OF INVESTIGATION (DDMMMYYYY):
26b. CLEARANCE LEVEL:	26c. IT LEVEL DESIGNATION □ LEVEL I □ LEVEL II □ LEVEL III

27. VERIFIED BY (Print name):	28. SECURITY MANAGER TELEPHONE NUMBER:	29. SECURITY MANAGER SIGNATURE:	30. DATE (DDMMMYYYY):

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

31. TILE:	31a. SYSTEM:	31b.ACCOUNT CODE:
	31c. DOMAIN:	
	31d. SERVER Bahrain	
	31e. APPLICATION: NCTS	
	31h. DATASETS:	
	31f. DIRECTORIES:	
	31g. FILES:	
32. DATE PROCESSED (DDMMMYYYY)	32a. PROCESSED BY:	32b. DATE (DDMMMYYYY):
33. DATE REVALIDATED (DDMMMYYYY)	33a. REVALIDATED BY:	33b. DATE (DDMMMYYYY):

INSTRUCTIONS

A. PART I: The following information is provided by the user when
establishing or modifying their USER IDENTIFICATION (ID).
(1) Name. The last name, first name, and middle initial of the user.
(2) Organization. The user's current organization (i.e., USS xx, DoD,and government agency or commercial firm).
(3) Office Symbol/Department. The office symbol within the current organization (i.e., SDI).
(4) Telephone Number/DSN. The Defense Switching Network (DSN) and commercial phone number of the user.
(5) Official E-mail Address. The user's official e-mail address.
(6) 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.
(7) Official Mailing Address. The user's official mailing address.
(8) Citizenship (United States (US), Foreign National (FN), Local National (LN), or Other), Identify appropriate citizenship in accordance with (IAW) SECNAV M-5510.30.
(9) Designation of Person (Military, Civilian, Contractor).
(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date of completion.

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

(11) 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.
(12) 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.)
(12a) If Block 12 is Privileged, user must sign a Privilege Access Agreement form. Enter date of when Privilege Access Agreement (PAA) form was signed. Users can obtain a PAA form from the Information Assurance Manager (IAM) or Appointee.
(13) User Requires Access To. Place an "X" in the appropriate box. Specify category.
(14) Verification of Need to Know. To verify that the user requires access as requested.
(14a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
(15) Supervisor's Organization/Department. Supervisor's organization and department.
(15a) Official E-mail Address. Supervisor's e-mail address.
(15b) Phone Number. Supervisor's telephone number.
(16) 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.
(16a) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
(16b) Date. Date supervisor signs the form.
(17) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.
(17a) Phone Number. Functional appointee telephone number.
(17b) Date. The date the functional appointee signs the OPNAV 5239/14.
(18) Signature of Information Assurance Manager (IAM) or Appointee. Signature of the IAM or Appointee of the office responsible for approving access to the system being requested.
(19) Organization/Department. IAM's organization and department.
(20) Phone Number. IAM's telephone number.
(21) Date. The date the IAM signs the OPNAV 5239/14 form.
(22) Standard Mandatory Notice and Consent Provision and User Responsibilities. These items are in accordance with DoD Memo dtd May 9, 2008 (Policy on Use of DoD nformation Systems – Standard Consent Banner and User Agreement) and DON CIO message Responsible and Effective Use of Dept of Navy Information Technology Resources" DTG 161108Z JUL 05.
(23) Name. The last name, first name, and middle initial of the user.
(24) User 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). User shall digitally sign form. Pen and ink signature is acceptable for users that do not have a Common Access Card (CAC) or the ability to digitally sign the form.
(25) Date. Date signed.

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

(26) Type of Investigation. The user's last type of background investigation (i.e., National Agency Check (NAC), National Agency Check with Inquiries (NACI), or Single Scope Background Investigation (SSBI)).
(26a) Date of Investigation. Date of last investigation.
(26b) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(26c) Identify the user's IT designation level. If Block 12 is designated as "Authorized" then IT Level Designation is "Level III". If Block 12 is designated as "Privileged" then IT Level Designation is "Level I or II" based on SECNAV M-5510.30 dtd June 2006.
(27) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(28) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.
(29) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.
(30) 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 OPNAV. This information will specifically identify the access required by the user.

(31 - 33b). Fill in appropriate information.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed or mailed. If the completed form is transmitted electronically, the e-mail must be digitally signed and encrypted.

FILING: Form is purposed to use digital signatures. Digitally signed forms must be stored electronically to retain non-repudiation of electronic signature. If pen and ink signature must be applied, original signed form must be retained. Retention of this form shall be IAW SECNAV Manual M-5210.1, Records Management Manual. Form may be maintained by the Navy, the user's IAM, and/or Security Manager. Completed forms contain Personal Identifiable Information (PII) and must be protected as such.

UNCLASSIFIED/FOUO

KVM (Keyboard Video Mouse) USER AGREEMENT

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the user of the KVM device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security policies. The information is used for inventory control of the device and to verify compliance with DoD requirements regarding accountability security requirements IAW Sharing Peripherals Across the Network Security Technical Implementation Guide (SPAN STIG) 3.1
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial to operate or use of the KVM.

PART I - PERSONAL INFORMATION

1. LAST NAME	2. FIRST NAME	3. MIDDLE INITIAL
4. RANK/RATE	5. ORGANIZATION	6. DEPARTMENT/DIVISION
7. BUILDING NUMBER	8. ROOM NUMBER	9. WORK TELEPHONE NUMBER
10. E-MAIL ADDRESS		

PART II - USER AGREEMENT – Standard Mandatory and Consent Provision

User Will:

- Ensure that the switches are approved before installing
- Ensure that the systems are installed correctly and meet all TEMPEST standards
- Ensure the desktop banners, backgrounds, and screen locks have the proper classification banner
- Protect the system and KVM in your area
- Report any spillage of classified information to your IAO or the IAM
- Safeguard and report any unexpected or unrecognized computer output, including both displayed or printed products
- Use different passwords on each system connected through a KVM
- Ensure that the classification level is displayed by each systems screen lock and that the password is required to regain entry to the system
- Ensure that the systems screen lock is invoked if the system is left unattended of if there is a 15-minute period of inactivity for each system
- Be responsible for marking/labeling magnetic media

Administrative Procedures: Users are required to follow the procedures below when using KVM switches:

1. Logon onto an IS.
    a. Identify the classification of the IS currently selected.
    b. Use the login and passwords appropriate for that IS.
    c. Verify the classification of the present IS by checking the classification label/banner.
    d. Begin processing.

2. Switching between ISs.
    a. Screen lock the IS you are currently using if the IS supports this capability.
    b. Select the desired IS with the switch.
    c. Enter the user identifier and password to deactivate the screen lock on the newly selected IS.
    d. Verify the classification of the present IS by checking the classification label/banner.
    e. Begin processing.

Physical Security Controls:

KVM switches are normally unclassified devices; however, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. For example, if the switch is connected to a classified system and an unclassified system, then it will be protected in the same manner as the classified system. Physical access to the KVM switch must also be restricted to individuals that are allowed physical access to all ISs attached to the system.

Labels:

All IS components must be labeled, including all switch positions. They must be clearly marked with the appropriate classification labels.

Desktop Backgrounds:

To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (Secret - red, Confidential - blue, Unclassified - green).

When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

Screen Locks:

Screen lock applications must display the highest classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.

Smart Keys:

Systems using KVM switches must not employ “smart” or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications. This includes keyboards with smart card readers, Universal Serial Bus (USB) ports, and removable media drives.

Hot Key Capability:

If the switch has configurable features, the configuration must be protected from modification by the user with a DOD compliant password.

Switches featuring the ability to automatically toggle between Information Systems (IS) must have this feature disabled. The only “hot key” feature permitted to be enabled is the menu feature that allows the user to select the IS to be used from a displayed menu.

Scanning Capability:

Switches with the ability to automatically scan and switch to different CPUs are prohibited.

Wireless or Infrared Technology:

Systems using KVM switches must not use keyboards or mice with wireless or infrared technology.

Connectors:

The use of switches to share peripherals other than the keyboard, video/monitor, and mouse by connecting peripherals to ISs of different classification levels is prohibited. All switches that are attached to ISs of different classifications will have this feature disabled. Regardless of whether it can be disabled, no peripheral devices other than the keyboard, video/monitor, or mouse will be connected to the KVM switch.

Connectors used for this feature will be blocked with tamper resistant seals. Additionally, all unused connectors for ISs will be blocked with tamper resistant seals. All cable connections will be marked with tamper resistant seals that allow visual confirmation that the configuration of the cable has not been modified.

Unique Password:

At a minimum, users must ensure that they use different/unique passwords for each system connected through a switch. System administrators should employ different logon USERIDs to help users further distinguish between the systems.

Training:

Periodic training is required to ensure that users are trained and in compliance with the requirements associated with the introduction and use of KVM switches.

FOR REPORTING PROBLEMS OR TO ASK QUESTIONS, CONTACT NCTS-ME Enterprise Service Desk (ESD): 439-6287

By signing this document, I acknowledge that I have read and understood my duties and responsibilities in relation to the use, operation, and information security requirements of the KVM switch.
a

12. SIGNATURE OF USER	13. DATE SIGNED (YYYYMMDD)

UNCLASSIFIED/FOUO