



DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

Ser 08Y/04-00682
14 May 04

From: Commander, Naval Sea Systems Command
To: Distribution

Subj: NAVY/MARINE CORPS INTRANET (NMCI) — ACTIVITIES PROCESSING
NAVAL NUCLEAR PROPULSION INFORMATION; REQUEST FOR ACTION

Ref: (a) DD 254, Amendment P00049 of Contract N00024-00-D-6000 of 12 Sep 02
(b) NAVSEA ltr 08Y/03-03586 of 20 Nov 03
(c) NAVSEA ltr 08Y/03-03976 of 12 Dec 03
(d) COMNAVNETWARCOM Norfolk VA msg 222000Z Dec 03

Encl: (1) NMCI — User Agreement for Users at NNPI Processing Activities Switched to
Classified NMCI Workstations
(2) NMCI — User Agreement Form for NNPI Processing Activities

1. **Background.** Under public law (e.g., the Atomic Energy Act of 1954, as amended), Naval Nuclear Propulsion Information (NNPI) must be protected from unauthorized disclosure to foreign nationals and other personnel who do not have an appropriate need to know. Reference (a) identifies the requirements for protecting either classified or unclassified NNPI that is transmitted over the Navy/Marine Corps Intranet (NMCI). NNPI will be protected on the NMCI networks (both classified and unclassified) through a community of interest (COI), which is a group of NNPI-approved users operating an NNPI-approved NMCI workstation while accessing NNPI.

2. NAVSEA 08 Discussion

a. Because of repeated failures in configuration control and quality assurance, reference (b) disapproved widespread deployment of the unclassified NNPI COI workstations. Reference (c) required that all NNPI processing activities continue to process NNPI on legacy networks, the existing non-NMCI networks, until a NAVSEA 08-approved NNPI COI is available. An exemption to the requirement allowed sites to process NNPI on the classified NMCI network if specific protective measures were implemented.

b. References (c) and (d) promulgated interim protective measures for NNPI processing activities that were switched from legacy networks to the classified NMCI network by the lead NMCI contractor, Electronic Data Systems (EDS), before the reference (a) contractual protections for NNPI were in place. However, the reference (d) requested interim NNPI protections on the classified NMCI network have not yet been engineered by EDS and the interim protections for handling NNPI on the classified NMCI network have had to be modified. Until the NNPI protections are engineered into the network, user operating procedures, not NMCI architecture, will be used to minimize the risk of unauthorized access to NNPI on the classified NMCI network. The most significant change to the reference (d) interim protective measures is the use of e-mail to share NNPI files instead of the use of special NMCI file folders for NNPI.

3. **Request for Action.** All activities that process NNPI are requested to complete the following actions:

a. Ensure all NNPI users that process NNPI on the classified NMCI network abide by the requirements described in enclosure (1) and sign the enclosure (2) user agreement form. The Information Systems Security Manager is responsible for maintaining signed forms. These forms will be made available to NAVSEA 08 or its designated representatives upon request. Activities are requested to report completion of this action by letter for all users at its site to NAVSEA 08 by 18 June 2004.

b. Ensure that unclassified NMCI workstations are not used for NNPI processing until NAVSEA 08 approved unclassified NMCI NNPI workstations are available. Activities that process NNPI will be on distribution for the correspondence providing NAVSEA 08 approval for deployment of NNPI workstations on NMCI.

4. The NAVSEA 08 point of contact on this issue is Mr. Todd Gordon, at telephone (202) 781.6202, or by email at <gordonrt@navsea.navy.mil>.

J. M. KLING
By direction

Distribution:

Commander, Naval Air Force, U.S. Atlantic Fleet
Commander, Naval Air Force, U.S. Pacific Fleet
Commander, Submarine Force, U.S. Atlantic Fleet
Commander, Submarine Force, U.S. Pacific Fleet
Commander, Portsmouth Naval Shipyard
Commander, Norfolk Naval Shipyard
Commander, Puget Sound Naval Shipyard & Intermediate Maintenance Facility
Commander, Pearl Harbor Naval Shipyard & Intermediate Maintenance Facility
Commander, Trident Refit Facility, Kings Bay
Commander, Trident Training Facility, Kings Bay
Commander, Trident Training Facility, Bangor
Commanding Officer, NPTU Charleston
Commanding Officer, NPTU Ballston Spa
NPEB CINCLANTFLT
NPEB CINCPACFLT
Naval Sea Systems Command Technical Representative, Schenectady
Naval Sea Systems Command Technical Representative, Pittsburgh
NAVICP (Codes 009, 87)

Copy to:

Director, Navy/Marine Corps Intranet
COMSUBPAC N4, N407
COMSUBLANT N4, N407
COMNAVAIRLANT N9, N43
COMNAVAIRPAC N9, N43
COMSUBRONs 1, 2, 3, 4, 5, 6, 7, 8, 11,
12, 15, 16, 17, 20, 22

COMDEVRON 5
COMSUBGRUs 1, 2, 7, 8, 9, 10
NRROs Groton, Norfolk, Newport News,
Portsmouth, Puget Sound, Pearl Harbor
ANNR San Diego, Kings Bay
Chief, West Milton Field Office

**NAVY/MARINE CORPS INTRANET (NMCI) — USER AGREEMENT FOR USERS AT NAVAL
NUCLEAR PROPULSION INFORMATION (NNPI) PROCESSING ACTIVITIES SWITCHED TO
CLASSIFIED NMCI WORKSTATIONS - UPDATED 14 MAY 2004**

1. Security Briefing.

a. *Purpose:* To emphasize individual responsibilities pertaining to all operation, administration, management, and control of NMCI or legacy information systems.

b. *General:* The protection of both classified and controlled unclassified information and data is based on the principles of individual responsibility, personal accountability and need-to-know. Information system security, like all other security disciplines, depends upon each individual.

c. *Responsibilities:* The responsibility for the protection of classified and controlled unclassified information and data used within NMCI and legacy information systems rests with each person. Regardless of countermeasures established to protect the confidentiality, preserve the integrity, or ensure the availability of sensitive computer systems, networks, or the data processed, they provide little security if ignored by individual users. The following NMCI and legacy Information System Security User Agreement outlines basic safeguards, which should be followed when using NMCI and legacy computer assets.

2. I understand that the user requirements for the NMCI and legacy information system security include the following:

a. I shall use only those NMCI and legacy information systems that I am authorized to access and only for the purpose for which they were intended.

b. My NMCI and legacy information system password(s) must be protected and may not be divulged to anyone.

c. I am responsible for my account use and determination of the correct classification of any file that I create, modify or manage.

d. When I gain access to NMCI or legacy information systems via non-NMCI workstations through remote access, I shall ensure that the information and data are protected in accordance with DOD, DON, and Privacy Act directives. This information must be protected at all times.

e. I shall not install any computer software or open an NMCI or legacy workstation to install computing equipment. Approved peripherals may be connected through available serial, parallel, or Universal Serial Bus (USB) ports.

f. I shall properly log off the NMCI or legacy information systems upon completion of the workday.

g. I shall use a password protected screen saver when departing the immediate terminal area for any length of time.

h. I shall not probe or attempt to break in or gain access to any computer system, or account that I am not authorized to access.

i. I shall exercise reasonable care in downloading and handling files from outside sources.

**NAVY/MARINE CORPS INTRANET (NMCI) — USER AGREEMENT FOR USERS AT NAVAL
NUCLEAR PROPULSION INFORMATION (NNPI) PROCESSING ACTIVITIES SWITCHED TO
CLASSIFIED NMCI WORKSTATIONS - UPDATED 14 APRIL 2004**

j. NMCI and legacy information systems are subject to authorized monitoring to ensure system functionality, verify the application of prescribed security countermeasures, and protect against unauthorized use. If monitoring reveals possible evidence of criminal activity, such evidence will be provided to law enforcement personnel.

k. Any attempt to circumvent NMCI or legacy information system security safeguards will result in immediate revocation of my information system access, adverse administrative action, and/or disciplinary action.

l. My local Information System Security Manager/Officer (ISSM/ISSO) is my primary point of contact for any problems or questions concerning NMCI or legacy information system security.

m. I shall immediately report any violation of NMCI or legacy information system security or any other inappropriate activity I observe or suspect to the local ISSM/ISSO. I must report any weakness in NMCI or legacy information system countermeasures or procedures I observe or encounter to the local ISSM/ISSO.

3. Naval Nuclear Propulsion Information:

Operational requirements are necessary for the protection of Naval Nuclear Propulsion Information (NNPI) on the classified Navy/Marine Corps Intranet (NMCI) network for personnel who have been switched to the classified NMCI network without the contractually obligated protections in place. These operating requirements are necessary to minimize the risk of unauthorized access to NNPI and will remain in effect until NAVSEA 08 provides revised guidance for processing NNPI on the classified NMCI network. Processing NNPI on any unclassified NMCI workstation is prohibited.

a. If I process Naval Nuclear Propulsion Information (NNPI), I affirm that (a) I am a U.S. citizen with the proper security clearance for the information I may handle; (b) my function in my command requires me to handle classified or unclassified NNPI; and (c) special handling controls are required to safeguard this information, including the following measures:

b. I am not permitted to process classified information on the unclassified NMCI or unclassified legacy information systems. I must report any occurrence of classified information discovered on the unclassified NMCI network or unclassified legacy information systems to the local ISSM/ISSO.

c. I am not permitted to process unclassified NNPI (U-NNPI) on the unclassified NMCI until the NNPI COI is approved and available at a workstation designated for my use. I may process U-NNPI on NAVSEA 08-approved legacy information systems identified by my command.

d. I am prohibited from processing NNPI on personally owned data processing systems.

e. I may process either U-NNPI or C-NNPI on the legacy Secure Internet Protocol Router Network (SIPRNet) workstations designated for my use if authorized by my command.

**NAVY/MARINE CORPS INTRANET (NMCI) — USER AGREEMENT FOR USERS AT NAVAL
NUCLEAR PROPULSION INFORMATION (NNPI) PROCESSING ACTIVITIES SWITCHED TO
CLASSIFIED NMCI WORKSTATIONS - UPDATED 14 APRIL 2004**

f. I shall adhere to the following practices and policy to process any U-NNPI or C-NNPI on classified NMCI seats before the C-NNPI COI becomes available on the classified NMCI network.

(1) To protect NNPI information on the local machine, I will create and use the following folder to store NNPI:

C:\Documents and Settings\{NMCI Userid}\My Documents\NNPI

(a) I shall not store NNPI in unencrypted locations on a workstation. Prohibited NNPI storage locations include the desktop and *Favorites*, which are replicated to the user's H drive on an NMCI file server.

(b) I shall follow guidance from my local command regarding backup requirements for these folders.

(2) I shall follow these steps to turn on Encrypted File Services (EFS) for the folder used to store NNPI:

C:\Documents and Settings\{NMCI Userid}\My Documents\NNPI

(a) In Windows Explorer, right-click the above folder, and then click *Properties*.

(b) On the *General* tab, click *Advanced*.

(c) Select the *Encrypt* contents to secure data check box.

(d) In the *Advanced Attributes* window, click *OK*.

(e) In the *NNPI Properties* window, click *OK*.

(3) I shall share files with other classified NMCI users exclusively via e-mail and shall ensure proper addressing for the intended recipient(s).

g. My local assistant customer technical representative, one of the NNPI COI officers, is my primary point of contact for any problems or questions concerning my authorization to access the NNPI COI.

h. I shall immediately report any violation of or other inappropriate activity for NNPI processing I observe or suspect directly to the local ISSM/ISSO and the NMCI help desk. I shall report any weakness in NNPI processing procedures or policy that I observe or encounter to the local ISSM/ISSO.

NMCI User Agreement Form for NNPI Processing Activities

This form acknowledges your receipt of, and agreement to comply with, the NMCI / Legacy Information Systems User Security Requirements, NETWARCOMINST 5239.1, the NMCI User Agreement for Users at NNPI Processing Activities Switched to Classified NMCI Workstations, and other policies and procedures for obtaining a network account.

PRIVACY ACT STATEMENT

USC V § 301 authorizes the collection of this information.

The principal reason we are asking for this information is to determine whether you are eligible for an NMCI/Legacy Network Account, an NMCI/Legacy Microsoft Exchange e-mail account, and/or Internet access. We may disclose this information to other authorized personnel, as necessary, to monitor and maintain your account. We may also disclose this information to a Federal, State, or local law enforcement agency if local activities or NMCI becomes aware of a violation or possible violation of civil or criminal law; or to a Federal agency investigating you for employment or security reasons. You are not required by law to give us this information; but if you chose not to, you will not be granted a user account.

Instructions

After reading the Naval Marine Corps Intranet/Legacy Information Systems User Security Requirements (version 1, dated 1 December 2003), NETWARCOMINST 5239.1, the NMCI User Agreement for Users at NNPI Processing Activities Switched to Classified NMCI Workstations, and the above Privacy Act statement, please provide the following required information. Then sign and date this form.

Type/Print Name: _____ **Social Security Number:** _____

Citizenship: U.S. citizenship required for NNPI access **Clearance:** Final Secret required for processing C-NNPI on Secret NMCI or SIPRNET

Command: _____ **Code:** _____ **Location:** _____

Acknowledgement

I have received and read a copy of NETWARCOMINST 5239.1, the NMCI and Legacy Information Systems User Security Requirements, the NMCI User Agreement for Users at NNPI Processing Activities Switched to Classified NMCI Workstations. **I UNDERSTAND MY RESPONSIBILITIES REGARDING ACCESS AND USE OF NAVAL MARINE CORPS INTRANET/LEGACY INFORMATION SYSTEMS AS SET FORTH IN THE ABOVE-REFERENCED DOCUMENTS AND AFFIRM THAT I WILL COMPLY WITH THE STATEMENTS, TERMS, AND CONDITIONS SET FORTH THEREIN.** I request access to the Naval Marine Corps Intranet/ Legacy Information Systems and Network Infrastructure, in order to conduct official work related to my position.

Signature: _____ **Date:** _____

Endorsement

U.S. Citizenship, Security Clearance, and need to process NNPI verified by:

Signature: _____ **Date:** _____

(Authorized NNPI COI Officer — CTR/DCTR/ACTR)

Legacy Information System Account User Name: _____
(To be completed by the Account Administrator)

NMCI Information System Account User Name: _____
(To be completed by the NMCI Account Administrator)

COPY TO BE RETAINED BY THE ISSM/ISSO