

MEMORANDUM

From NUWC POC:

Via: Dept. Information Systems Security Officer (ISSO)

Department ISSO Signature

To: Information Systems Security Manager (ISSM), Code 1043

Subj: **NMCI OWNED COMPUTER EQUIPMENT BROUGHT ONBOARD BY GOVERNMENT PERSONNEL**

1. Identification. Request the following individual be authorized to transport an NMCI computer as identified below, in and out of NUWCDIVNPT:

Name of Individual:

Agency:

Arrival Date:

Departure Date:

Bldg/Rm/Lab:

NUWCDIVNPT Point of Contact:

Code:

Telephone Ext.:

NMCI Asset Tag#:

Embedded Wi-Fi:

Yes

No

Additional Comments: **Use of Wi-Fi (802.11) is not permitted at this facility. User may connect to authorized NMCI Hotel Ports to access the NMCI network.**

2. Access. The personnel identified in paragraph 1 must keep a copy of this request with the computer equipment at all times while on board NUWCDIVNPT.

3. Operation. Unclassified NMCI computers are NOT allowed in classified spaces unless approved by the ISSO. All computer operations will be unclassified. Connection to any classified information system or network is prohibited. All wireless capability will be disabled or card removed prior to entry to NUWCDIVNPT. No web cameras, external or built-in, are permitted aboard NUWCDIVNPT. Full Disk Encryption is required for processing and storage of FOUO/CUI Government data and information.

4. Responsibility. The Government assumes no responsibility for lost, stolen or damaged computer equipment.

User (Non-NUWC) Signature

NUWCDIVNPT POC Signature

Approval:

Information Systems Security Manager

Date: