PORTABLE STORAGE DEVICE MEDIA AUTHORIZATION

From: Information Assurance Security Division (code 72600) Information Security Manager (IAM)

Subj: Authorization to Use a Portable Storage Devise (PSD) on the Navy Marine Corps Intranet (NMCI) Network at FRCSE

Ref: (a) DoD 5400.11-R Department of Defense Privacy Program
(b) DoDD 5400.11 DoD Privacy Program
(c) DON CIO Message 091256Z OCT 07 - DON Encryption of Sensitive Unclassified Data At Rest Guidance
(d) Protecting PII on Removable Storage Devices, By DON CIO Privacy Team, February 25, 2010

1. Your request to use one PSD on the NMCI Network is approved. This authorization applies only to the PSD and NMCI asset listed below at FRCSE. No other type of PSD will be allowed to be connected without the IAM (code 72600)/Assistant IAM consent.

1. NMCI PC NAME	2. HARD DRIVE NAME	3. MODEL #	4. SERIAL #

2. Before the drive can be reconnected to a Department of Defense (DoD)/ Department of the Navy (DON) network or system, it must be scanned for viruses, malware, spyware, and other known vulnerabilities at home and immediately before connecting to the NMCI network. This will help prevent the introduction of vulnerabilities into DoD/DON networks and systems.

a. Open Windows Explorer, right-click on the drive letter of your PSD, and select 'Scan for Viruses'.

b. Any possible malicious code contamination will be listed in the result window. **If a virus is detected, DO NOT TURN OFF THE COMPUTER**. **UNPLUG THE NETWORK CABLE FROM THE WORKSTATION CONTACT THE IAM (CODE 72600) IMMEDIATELY**. No result in the scan window after the scan completion is an indication of a Non-Contaminated USB Hard Drive/PSD.

3. In the event that a virus is detected on your NMCI workstation originating from your PSD, the PSD will be confiscated and use of any other PSD will not be allowed.

4. This authorization is in effect for the period of one year from the date of signature.

5. Adhere to the following conditions:

a. Only store work related and Sensitive Unclassified data in the PSD

b. Encrypt and verify that all data stored in the PSD is encrypted.

c. Safeguarde the data and secure it by removing the PSD from the computer/workstation when leaving, whether for a short period and for extended periods.

d. **IMMEDIATELY** report lost or stolen PSD to the IAM (code 72600).

e. Store PII data per DoD, DON/Local Command Directives, Regulations, Polices, etc.

ACKNOWLEDGEMENT

I have read and understand the responsibilities given to me as being a user of a Mobile Device and/or PSD. I also understand that the failure to meet these requirements will be reported and will result in confiscation of the PSD.

5. USER NAME - LAST, FIRST, M.I. *(print or type)*	6. CODE	7. PHONE NUMBER

8. USER SIGNATURE AND DATE	9. IAM (CODE 72600) SIGNATURE AND DATE

FRCSE 5512/1 (REV. 6/2012)

All fields required.
Complete all required fields and mark unused optional fields with N/A.

PRINT