



Personal Digital Assistant (PDA) NMCI Policy

***Derek Duchein
derek.duchein@navy.mil
(858) 537-8942 (Integrated Support Center)***

- **COMNAVNETWARCOM msg 051645Z Dec 03/NIA 12-03**
- **Navy only advisory.**
- **Establish DAA policy on PDA hardware, software, and peripherals.**
- **Policy applies to all Portable Devices that can be connected to a network.**
 - **Hand-Helds, Palm-Tops, Blackberries, or similar devices.**
 - **Applies to all Navy activities receiving NMCI services.**
- **Policy pertaining to wireless devices and other portable devices is DoD directive 8100.2 (14 Apr 04)**

- **Four classes of PDAs:**
 - **Palm Operating System (Palm OS) (Palm, Sony, CLIE).**
 - **Pocket PC/Windows CE (COMPAQ, HP, Toshiba).**
 - **Blackberry (includes transport and services).**
 - **Other OS (Sharp, Franklin).**

- **PDAs have a wide variety of accessories**
 - **Modems, Synchronization Cables, Wireless Connections, Cameras, Voice Recorders, and Flash Memory Storage.**

- **It is essential these personal productivity tools function IAW network security guidelines.**

- Applies to all portable/wireless PDA devices regardless of manufacturer or operating system.
- Specifically covers all PDAs intended for connection to NMCI whether in AOR, Cutover, or Steady State.
- Whether owned by the Government, a Contractor, or an Individual.
- Does apply to PDAs connected to non-NMCI networks.

■ Connection Approval

- ❑ Only DAA approved PDAs for a specific network can connect to a government machine on that network (NMCI approved PDAs are not authorized on BLII).
- ❑ The approval to add PDAs to the authorized list for a specific network
 - Must complete the Certification and Accreditation Process.
 - PDAs must be included the network's SSAA.
- ❑ Contractor owned PDAs are authorized to connect provided:
 - They are on the approved list of devices.
 - They are authorized by the local command.
 - They are included in the associated Statement of Work (SOW).
 - They will not be connected to contractor network.

■ Connection Approval (continued)

Personally owned PDAs **May not** be connected to NMCI network at any time.

■ Sharing Data

PDAs shall Hot-Sync or otherwise connect only with machines on approved networks.

- NMCI Hot-Sync cradles are connected to specific machine.

An approved PDA that has connected to a Navy network **may not** connect to a non-government machine.

“Hot-docking” between a government machine and a contractor owned network asset or a personal machine is **prohibited**.

■ E-Mail

E-mail **Shall only** be transferred to “Non-Blackberry” PDAs via Hot-Sync with an authorized computer / mail account.

■ Additional Guidance

Data exchange via wireless technology is addressed in the DoD wireless policy (DoD Directive 8100.2 of 14 Apr 2004).

Blackberry devices with voice capability may be used for unclassified E-Mail exchange provided voice and data exchange **do not** transmit at same time.

■ Authorized Data

PDAs approved for use on the Navy’s unclassified networks **may not** hold classified data.

Passwords, PINs, Combinations and other forms of User Identification will not be saved to a PDA.

■ Controlled Spaces

The introduction or use of PDAs in areas where classified information may be discussed or processed will be IAW with DoD Policy governing those spaces.

■ PDA Software

Only approved and licensed software is authorized for use on PDAs.

Requests for additional PDA software on the NMCI network must follow NRDDG processes.

■ Peripherals

Only peripherals specifically authorized in the IATO shall be used with any PDA that connects to a Navy network, regardless of actual connection status.

Shall only be used in the manner specified in the IATO.

■ Physical Security

- Unclassified PDA shall be controlled in a manner to prevent**
 - Intentional or unintentional data disclosure.
 - Tampering by unauthorized personnel.
- Use of Classified PDA**
 - Requires written local IA Approval Authority (formerly site DAA)
 - Only to support specific circumstances
 - NO “General Classified PDA” is allowed.
- At a minimum, the password option will be used when the PDA is shut off or locked, and a password is required on restart.**
- Unauthorized personnel shall not be allowed to use or borrow a government PDA.**

■ Physical Security (Continued)

□ An empty cradle attached to a computer can be used to clone a PDA, therefore users must:

- Physically disconnect and secure cradle when not in use, or
- Log out when the computer is unattended.
- *Locking out the account with the machine logged on is not sufficient to prevent cloning.*

□ Classified PDAs shall be properly labeled to identify the highest classification of data held and when not in use, physically secured in a GSA approved container to avoid unauthorized use or theft.

■ Physical Security (Continued)

□ Additional Information

- Use of a PDA does not require an individual IATO/ATO.
- the Site SSAA must describe the use of PDAs and ConOps for protected information residing on the PDA.
- As new technologies emerge, the policy will be updated to ensure appropriate protections exist.
- Questions or concerns relating to PDA use and policy should be directed to NETWARCOM DAA Staff.



PDA Issues (Tabled at May S/TEAG)



Description:

- The current NMCI PDA NIA considered too restrictive by DON. An updated PDA policy and guidance for NMCI is needed. Policy to include PDA approved capabilities and mode of operations.
- Provide to SHC a list of approved PDA devices.

Impact:

- Claimants committed to PDA technologies will need to program for standards based PDA use.

Status: (as of 20 Feb 04)

- Actions completed to date or are currently in progress
 - PDA Policy NIA released DTG 051645ZDEC03
 - CLN 23 provides approved list of devices as follows (Palm 5, Palm M515, Blackberry NEXTEL 6510 and RIM 957-8)
- Next Step (30 days out)
 - EDS/PMW 161/ NETWARCOM/USMC to provide PDA capabilities stmt
- Timeline with Major Milestones identified
 - NETWARCOM/ USMC DAA to review USMC PDA Policy.(MAY04)
 - NETWARCOM to release updated PDA (possible Joint) policy based on capability statement. (JUN04)

Responsible Actionee(s):

- NETWARCOM: Bob Turner, (757-417-6776, bob.turner@navy.mil)
- PMW 161 Colin Purdy