



DEPARTMENT OF THE NAVY  
COMMANDER NAVY REGION SOUTHWEST  
937 NO. HARBOR DR.  
SAN DIEGO, CA 92132-0058

IN REPLY REFER TO :

COMNAVREGSWINST 5238.2  
N60  
11 FEB 2002

COMNAVREGSW INSTRUCTION 5238.2

Subj: PERSONAL DIGITAL ASSISTANT (PDA) INSTRUCTION FOR  
CLASSIFIED AND UNCLASSIFIED ENVIRONMENTS

Ref: (a) CINCPACFLT Personal Digital Assistant (PDA) Policy  
for Classified and Unclassified Environments  
(b) Department of Defense 14 Jul 00  
(c) Department of Defense 21 Mar 88  
(d) Secretary of the Navy 17 Mar 99  
(e) Department of Defense 10 Feb 98  
(f) Joint DODIIS/Cryptologic SCI Information Systems  
Security Standards CH-15 31 Mar 01  
(g) Department of the Navy Jul 94  
(h) FLTINFOWARCEN RMG 131301Z Jul 01  
(i) CNO RMG 272200Z APR 01  
(j) SSO DIA RMG 211900Z MAR 01  
(k) Director of Central Intelligence Directive Jun 99

1. Purpose. The purpose of this instruction is to define Personal Digital Assistants (PDAs), stipulate under what conditions they can be connected to a PACFLT network, and how the information (both unclassified and classified) must be stored, processed, transmitted and protected. In addition, this instruction outlines how these devices will be protected commensurate with the computing environment in which they are operating. Use of PDAs within a Sensitive Compartment Information Facility (SCIF) requires additional security standards addressed in paragraph 6.

2. Background. PDAs (e.g. Palm Pilot) are a small subset of Portable Electronic Devices (PEDs). These hand-held devices have the ability to process, store, and transmit information between similar devices and other PEDs as well as Personal Computers.

3. Scope

a. This instruction applies to all Pacific Fleet subordinate commands.

11 FEB 2002

b. This instruction provides minimum guidelines for the use of PDAs for CINCPACFLT claimant activities. Individual Designated Approval Authorities (DAA) are authorized to impose more restrictive guidelines based on operational requirements and evaluated risk.

c. This instruction applies to all government owned/purchased commercial-off-the-shelf (COTs) PDAs using the Palm Operating System (PALM OS) (i.e., Palm Pilot, Handspring Visor or the Blackberry (RIM) operating system) that connects to a fleet network asset and/or are used to process, store, or transmit unclassified (including For Official Use Only) or GENSER classified information up to and including TOP SECRET. PDAs using other operating systems such as the Windows CE (Compaq, HP Jornada, Casio, etc.) are not authorized to be connected to a fleet network asset or to process, store, or transmit "For Official Use Only" and/or classified information.

(1) For the purpose of this instruction, government owned/purchased is defined as those devices that have been procured by a DOD agency for official use. This includes but is not limited to devices procured by CINCPACFLT claimant activities, service schools, and academies. Contractor owned PDAs are defined as privately owned, with the exception of those PDAs that are included in the Navy Marine Corps Intranet (NMCI) contract.

d. This instruction does not apply to other types of portable electronic devices such as laptop/notebook computers, pagers, two-way radios, audio/video/data recorders, mobile/cellular telephones, or digital cameras (still/video). Instructions governing use of these PEDs will be generated via separate correspondence.

e. This instruction will be reviewed annually to ensure compliance with evolving DOD and navy portable electronic device policies and commercial technologies.

#### 4. Purchasing PDAs

a. All PDAs must be pre-approved by Regional Information Technology Service Center (RITSC) prior to purchase.

b. Documentation of approval must be in the form of an authorized signature on the purchase card procurement request or an email from the authorizer, which is then attached to the procurement request.

11 FEB 2002

b. The procedures outlined in chapter 9 of reference (d) for transferring GENSER classified material will be followed for PDAs used to process, store, or transmit GENSER classified material up to and including Top Secret. Unless there is an urgent operational requirement, GENSER classified PDAs will not be hand-carried between duty stations. If an urgent operational requirement exists, the procedures outlined in reference (d), chapter 9 will be followed. This includes but is not limited to:

(1) Using a locked briefcase as an outer covering as long as the GENSER classified PDA is not being hand-carried on a commercial aircraft.

(2) Ensuring the PDA is never left unattended.

(3) Storing the PDA at a U.S. Embassy, military or appropriately cleared DOD contractor facility during over night stops.

(4) Never storing the PDA in vehicles, hotel rooms or hotel safes.

(5) Ensuring the command ISSM/ISSO or DAA has provided written authorization to all individuals hand carrying GENSER Top Secret and below PDAs. A DD 2501, Courier Authorization Card or Official Travel Orders, Visit Requests or Courier Authorization Letter are acceptable.

#### 11. Installation of PDA software

a. Per reference (g), personally owned software will not be loaded onto a government owned PDA unless the DAA has established procedures for the installation and the individual has agreed to abide by licensing agreements.

b. Any government owned software used on a PDA would be used per the specific licensing agreements for that specific software.

c. For shore commands, no software will be loaded to the GENSER classified or unclassified network to support a PDA without prior approval of the DAA. Any software that is approved for installation must be documented in the current System Security Authorization Agreement (SSAA) for the site/system per reference (e).

in any Sensitive Compartmented Information Facility (SCIF) is prohibited.

i. PDAs inside SCIFs are subject to DIA/SSO Navy/Regional SSO inspection at any time. The introduction of unauthorized classified information to a PDA will result in a security violation. The PDAs are subject to confiscation if classified information is discovered and/or must be controlled at the higher, more restrictive level.

#### 8. INFOCON Impact

a. At INFOCON CHARLIE, review options and impacts of disconnecting all PDAs from GENSER classified and unclassified networks and using in stand-alone mode only. Disconnect all non-mission critical PDAs from GENSER classified and unclassified networks.

b. At INFOCON DELTA, disconnect all PDAs from GENSER classified and unclassified networks.

#### 9. Storage and Destruction

a. Individuals assigned PDAs must exercise prudent care to ensure the device is not lost or stolen.

b. Per chapter 10 of reference (d), PDAs used to process, store or transmit GENSER classified information that are not under the personal control or observation of an appropriately cleared individual shall be guarded or stored in a locked GSA-approved security container, vault, modular vault, or secured room approved for open storage.

c. There is no formal guidance on PDA declassification. Therefore, physical destruction is currently the only method available to declassify a PDA that was used to process, store or transmit GENSER classified information or has been connected to a GENSER classified network or PC.

#### 10. Transporting PDAs

a. Only PDAs that are used to process, store, and/or transmit unclassified information can be hand-carried and do not have to be continuously maintained in a government facility. Individuals are authorized to take these devices home. As with any government issued item, care should be taken to ensure the devices are not lost or stolen.

11 FEB 2002

7. Use in Sensitive Compartmented Information Facilities (SCIF)

a. Per references (f) through (k), the use of PDAs in a SCI environment presents an unacceptably high degree of risk for the compromise of classified or sensitive information.

b. Per references (f) through (k), government PDAs are prohibited from operating within a SCIF unless authorized and approved for co-location by the appropriate SCI DAA or DAA Representative, i.e. via sys-4/SSO Navy-521 for ships and via shore-based accredited SCIFs, and NAVSECGRU for NSG-accredited SCIFs.

c. Per reference (f), connection of a government PDA to any GENSER information system within a SCIF must be approved by the command DODIIS/SCI ISSM. Ship SCIFs accredited by DIA/SSO Navy must notify SSO Navy-521 when this occurs.

d. PDAs cannot be used to process or store SCI data since these devices are currently not configurable to meet the minimum-security requirements outlined in reference (k) chapters 4, 5 and 6. Per references (f) and (g), PDAs storing GENSER classified information will have their wireless, Radio Frequency (RF), microphones, and recording capability disabled (either by hardware or software).

e. PDAs and associated media must be transported and stored in a manner that affords security sufficient to preclude compromise of information, sabotage, theft or tampering. Procedures for handling the PDA in a SCIF must be available and provided to the user.

f. PDAs operating within a SCIF will have their wireless, RF, microphones and recording capability disabled (either by hardware or software).

g. The Infrared (IR) capability will not be used to transmit or receive information from another PDA or device while a PDA is physically connected to any network or PC (classified or unclassified). If existing SCIF systems utilize IR capability, then the PDA IR capability must be disabled. If IR capability is not being used in the SCIF for other purposes the appropriate SCI DAA, DAA Rep or DODIIS/SCI ISSM for use in the SCIF can approve the PDA IR capability for use.

h. The connection of unclassified government owned PDAs to any classified electronic device; network or information system

11 FEB 2002

(2) If the PDA was used for GENSER classified material, up to and including Top Secret, the procedures outlined in chapter 9 of reference (d) for transferring GENSER classified material will be followed. Unless there is an urgent operational requirement, GENSER classified PDAs will not be hand-carried between duty stations. If an urgent operational requirement dictates that a GENSER classified PDA be hand-carried between duty stations, the procedures outlined in reference (d), chapter 9 will be followed.

d. For individuals departing the navy, that have been assigned PDAs purchased by other military organizations, the PDA will be returned to their current command's ISSM/ISSO for appropriate disposition.

#### 6. Connection to a CINCPACFLT network

a. No personally owned PDAs will be connected to any government personal computer (PC) or network.

b. Prior to connection of any PDAs to any networked computer, the command must ensure that this connection is identified in the System Security Authorization Agreement (SSAA) per reference (e) and is approved by the responsible DAA. In addition, for connections to a Secret Internet Protocol Router Network (SIPRNET) workstation, the accreditation documentation must be updated to reflect the connection and the connection approval process must be updated.

c. Once a PDA is connected to a PC or network, it assumes the highest classification level the PC or network is approved to process, store or transmit information. Since there are no approved methods to downgrade the classification of PDAs, once connected to a classified PC or network, the PDA cannot be connected to a PC or network of a lower classification level (i.e., a PDA connected to a SIPRNET computer cannot be connected to a Non-secure Internet Router Network (NIPRNET) computer). In the event of an inadvertent connection of a GENSER classified PDA to a PC or network of a lower classification, the command ISSM/ISSO must be notified immediately. In addition, the Site Security Officer (SSO) must be notified immediately if a PDA is inadvertently connected to a Sensitive Compartmented Information (SCI) network.

11 FEB 2002

CINCPACFLT network or can be used to process, store and/or transmit official unclassified or GENSER classified information: The command ISSM/ISSO will ensure that the device is logged into the personal property accounting system. If the device and/or hotsync cradle does not contain a classification sticker, it will be added.

(3) In addition to the procedures outlined in paragraph 5.a.(1) above, for PDAs used to process, store and/or transmit Top Secret information, each PDA will be individually serialized, entered into the command's Top Secret log, and be physically sighted or accounted for annually per reference (d).

b. PDAs and/or hotsync cradles purchased by CINCPACFLT claimant activities will be returned to the command ISSM/ISSO prior to the individual departing the command with the following exceptions, PDAs purchased by Commander, Navy Region Southwest (CNRSW) for NRSW civilian employees stay at NRSW when the civilian employee departs. PDAs purchased by CNRSW for NRSW military personnel can be taken by the military employees when they depart provided the PDAs were for unclassified materials only. Local departments/programs are responsible for collecting PDAs at the military member's/employee's checkout. Any PDAs purchased by CNRSW and used to process, store and/or transmit classified information will remain at NRSW when civilian or military personnel depart. **No exceptions.**

(1) Per reference (b), all government owned/purchased PDAs will be cleared of all data by RITSC and inspected by RITSC to ensure all information has been completely removed prior to reassignment of the device to another user.

(2) Currently, there are no approved methods for downgrading the classification of PDAs. Therefore, when the device is reissued, the individual must have the appropriate or higher level clearance than the classification of the PDA. The PDA will continue to display the classification marking of the highest classification of data that has ever been on the PDA.

c. For PDAs and/or hotsync cradles purchased by other military activities, the individual can be allowed to take the PDA and/or hotsync cradle when they transfer from the command to another military command per the procedures below:

(1) The device must be returned to the command ISSM/ISSO so it can be removed from the command's personal property inventory.

11 FEB 2002

c. Once RITSC approves the procurement of the PDA, RITSC notifies the local Regional Property Coordinator in the local Resource Management Office (N80).

d. Regional Property Coordinator will notify the appropriate department/program property coordinator for subsequent entry into Defense Property Accountability System (DPAS).

e. Once a PDA is received by a user, the user must:

(1) Contact property coordinator to assign/apply barcode to PDA and enter into DPAS.

(2) Contact local Information System Security Officer (ISSO)/Information System Security Manager (ISSM) to assign security level and apply classification sticker. Local ISSO/ISSM will ensure property logged into DPAS.

(3) Contact RITSC for connection/loading software. RITSC will not load software unless all of the following have been accomplished: RITSC has given approval for purchase (if purchased by this command), barcode is assigned, and security level/classification sticker is applied.

## 5. Controlling PDAs

a. Per references (b) and (c), all government owned/purchased PDAs will be assigned to an individual, by name and organization, and will be tracked as part of the organizational inventory.

(1) PDAs purchased by CINCPACFLT claimant activities for use in the UNCLASSIFIED and GENSER CLASSIFIED environment, up to and including SECRET will be logged into a personal property accounting system by the local property coordinator of the department/program purchasing the PDA. Per reference (d), a classification sticker, indicating the highest classification level of information that can be stored, processed or transmitted, and the local ISSM/ISSO and the corresponding hotsync cradle will place a U.S. government property label on the PDA.

(2) For PDAs issued by other military commands, the following must occur before the device can be connected to a

11 FEB 2002

d. For afloat commands, no software will be loaded to the Integrated Shipboard Network System (ISNS) LAN unless it is reflected in the SPAWAR Functional Baseline Configuration (FBC) or is reflected on the Preferred Product List (PPL). Reference (j) provides guidance for proposing software for inclusion on the PPL.

e. Blackberry devices are authorized for use on unclassified networks only due to their inherent wireless capability. Commands desiring to implement use of Blackberry devices should contact the CINCPACFLT FITSC (Mr. Garrett Chew 808-471-3115, chewgl@CPF.navy.mil) for technical guidance.

12. Reporting loss of PDA. All PDAs that are lost or stolen must be immediately reported to the command ISSM/ISSO. The command security manager must also be notified if the PDA was used to process, store and/or transmit GENSER classified information or was connected to a GENSER-classified network. DD form 200 must be completed to document loss and request removal of asset from DPAS.

13. User awareness and training. Commands that issue PDAs to process, store and/or transmit unclassified or GENSER classified information must incorporate information concerning the requirements of this instruction as well as the risks associated with these devices into their user awareness training.

  
D. C. KENDALL  
Deputy and  
Chief of Staff

Copy to:  
[www.cnrsw.navy.mil/admin/menu.htm](http://www.cnrsw.navy.mil/admin/menu.htm)