National Nuclear Security Administration

NNSA Policy Letter: BOP-65.001
Date: September 7, 2007

TITLE: Issuance and Usage of Portable Computing and Communications Devices (PCCD)

I. OBJECTIVES

This policy governs the issuance and usage of Portable Computing and Communication Devices (PCCDs). A PCCD is any portable electronic device that stores NNSA data and has the capacity to: a) be used off site; b) access NNSA data while off site; or c) connect to NNSA networks while off site. Such devices include, but are not limited to laptop computers and PDAs. This definition does not include external storage devices or desktop computers.

The objectives of this policy are to:

- Set forth the expectations of the NNSA regarding the protection of NNSA data present on, processed by, or accessed through any computing or communications device by an NNSA affiliated user while at any location.
- Reduce the risk associated with loss of Federal property and sensitive information.
- Reduce the overall costs associated with acquiring PCCDs and associated communication services.
- Ensure that PCCDs are used consistent with the signed user agreement.
- Provide a consistent, understandable, repeatable, and enforceable basis for providing PCCD services for NNSA Federal personnel.

II. APPLICABILITY

A. General. This policy applies to:

1. All NNSA Federal employees that have been issued PCCD by either the Federal government or by a contractor to the Federal government, and
2. PCCDs issued by an NNSA element to contractor employees.
3. Any personal PCCD used by NNSA Federal employees to conduct the business of the NNSA.

Where requirements and responsibilities apply to particular organizations within the complex, the applicability is explicitly stated. Policy will be published in the future to mandate NNSA contractor requirements regarding the issuance and usage of PCCDs. This policy pertains to all types and categories of unclassified processing, including sensitive unclassified information.

B. Exclusions. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Policy for activities under the Deputy Administrator's cognizance.

III. REQUIREMENTS

A. Issuance at NNSA Facilities.

1. A PCCD must be assigned to a single person either on a permanent or temporary basis. If a PCCD will have multiple users they all must sign the user agreement. A single individual must be assigned as responsible for the PCCD.
2. Users must accept and sign the user agreement (see Attachment 2) prior to issuance of PCCD.
3. A requestor may not concurrently have both a desktop computer and permanently-assigned laptop computer, nor a PDA and laptop computer, nor a cell phone PDA and cell phone concurrently, unless justified and approved by a senior manager. Criteria for justification includes:
   a. An identifiable critical mission requirement,
   b. A requirement for an employee to work after hours or outside their normal duty station,
   c. A requirement for an employee to work on an independent project requiring a PCCD.
4. All manner of approvals related to issuance of PCCDs must be recorded in a manner that facilitates reporting.
5. The requestor must specify a programmatic business need for the requested PCCD.
6. The request for a PCCD must specify a date of return, consistent with the category under which the request is made.
7. Assignments of PCCDs must be reviewed and validated, and user agreements re-signed, on an annual basis.
8. The assignment of PCCDs may be limited based on budget and availability.
9. NNSA program offices, staff offices, site offices and the Service Center may further restrict PCCD issuance and control.
10. Categories of Assignment. The assignment of a PCCD must be made under one of the categories specified below.
    a. Category 1A. Assigns a PCCD for an indefinite period to members of the Senior Executive Service (SES), without requiring management approval.
    b. Category 1B. Assigns a PCCD for an indefinite period, as approved by a senior manager, where the position description (or statement of duties) of the requestor meets one of the following criteria:
       - Supports Emergency Response, Emergency Management or Emergency Operations Support during deployments and events.
       - Is "on-call" staff (e.g., IT Support, COOP, or flexible location staff) for more than 20 hours per week.
       - Has an after-hours work requirement occurring more than 20 hours per week.
       - Has a travel requirement or out-of-building requirement greater than 12 hours per week.

- Supports the response to threatened or actual acts of terrorism.

c. Category 2. Assigns a PCCD from 31 to 90 days, as approved by a senior manager, where the requestor's job assignment (not position descriptions or statement of duties) is one of the following:

- Temporary duty station (i.e., travel, outgoing detail, etc) lasting from 31 to 90 days; or
- Other temporary assignment, as deemed necessary by the conditions of the assignment.

d. Category 3. Assigns a PCCD for up to 30 days, as approved by a line manager, where the requestor's job assignment is one of the following:

- Temporary duty station, lasting 30 days or less; or
- Other temporary assignment, as deemed necessary by the conditions of the assignment.

B. Security For All NNSA PCCDs And For Personal PCCDs That Contain NNSA Data.

1. PCCDs must be managed in accordance with the requirements defined in NAP-14.2-B (see Attachment 3 for excerpts from NAP 14.2-B). NNSA program offices, staff offices, site offices and the Service Center may add additional security requirements to protect PCCD.
2. When not present on site, external storage devices that store sensitive unclassified information must be encrypted in accord with FIPS140-2.
3. Access to a PCCD must be controlled by a password capability, which the user may not disable.
4. PCCD passwords must meet the standards set forth in NAP-14.2-B; PDA passwords are exempt from the requirement of NAP 14-2.B pertaining to special characters.
5. PCCDs must have a screensaver set and a requirement to re-enter the user's password after no more than 10 minutes of inactivity. User may set this timeout to a lower value.
6. Remote access to any NNSA or DOE services requires two-factor authentication where one of the factors is provided separate from the computer gaining access (e.g., RSA token or your fingerprint, in a biometric solution); PDAs are exempt from this requirement.
7. Any PCCD containing NNSA information must have all that data encrypted in conformance with FIPS 140-2.
8. When taken from an NNSA site, an unattended PCCD must be secured in such a manner to reasonably prevent the loss or theft of the device.
9. Any wireless capability is disabled (e.g., by user selected off switch or inert plug in of the mic port) during NNSA operations unless specifically authorized in accordance with NAP-14.2-B.
10. Any audio recording capability is disabled unless specifically authorized by the facility cyber security office.

11. Software installed on the government owned/issued PCCD must be authorized by line management and the system support Help Desk, and be consistent with the applicable Cyber Security Program Plan (CSPP).

C. Privacy. Users have no explicit or implicit expectation of privacy. The NNSA retains the right to monitor any and all uses of this communications system for any waste, fraud, or abuse.

D. Limitations.

1. Unauthorized or improper use of a PCCD may result in administrative disciplinary action and civil and criminal penalties, consistent with DOE O 3750.1, 5 CFR, and US Code, Title 18.
2. The extent of personal use, along with the expectations regarding privacy, is defined more fundamentally and in detail in DOE O 203.1.
3. If PCCD is unable to support encryption and password protection, it may not be taken off-site.
4. All distribution and uses of PCCDs, other than those prescribed here, are prohibited.

E. Foreign Travel. All PCCDs, except PDAs and emergency response PCCDs, used for foreign travel must:

1. be supplied from a separately managed pool of loaner PCCDs.
2. be provisioned with a standard software and hardware configuration, as determined by site requirements;
3. be provisioned in a manner that does not violate the laws of the destination or export control laws of the United States;
4. be provisioned and imaged in a manner that enables detection of physical and logical tampering; and
5. upon return, including external storage devices, undergo an inspection for tampering (both physical and logical) prior to being attached to an NNSA network, and/or before being re-issued.

F. Management and Oversight

1. Monitoring for Waste, Fraud, or Abuse.
   a. Data on a PCCD may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, DOE, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign.
   b. Upon detecting waste, fraud, or abuse, and without warning, the NNSA may terminate the PCCD service and retrieve the PCCD, in accord with established Departmental policy.
   c. The NNSA may perform utilization monitoring, randomly or with cause.
2. Handling Lost, Stolen, or Damaged Property. PCCDs that are lost, stolen, or damaged will be handled in accordance with the user agreement and DOE O

580.1, including its implementing guidance, which details possible personal financial liability.

3. Implementation. Within two weeks after publication of this directive, NNSA Elements shall provide the NNSA Chief Information Officer with a plan to implement the requirements of the Policy by September 28, 2007. The plan must include timelines and resources needed to fully implement this Policy.

G. Exceptions

1. The NNSA CIO, Site Office Managers, and the Director of the Service Center may authorize exceptions to these Requirements, in a manner consistent with DOE M 251.1B.

IV. RESPONSIBILITIES

A. NNSA HQ Programmatic and Staff Offices, Site Office Managers, and the Service Center Director must:

1. Take all practical measures to assure the security of NNSA information that is stored on, processed by, or transmitted through an NNSA-issued or operated PCCD as specified in NAP-14.2-B
2. Consistent with this policy, issue PCCDs in a manner that reduces overall cost and risk to property and information.
3. Ensure that the assignment and continued use of each PCCD is documented and justified by an approved programmatic business need.
4. Ensure that NNSA-issued PCCDs are used in accord with a user agreement.
5. Ensure that users of PCCDs are trained to employ the devices and execute their responsibilities stated in this Policy.
6. Ensure that records are kept of the procurement of PCCD.
7. Ensure that a semi-annual inventory is conducted and reconciled.
8. Ensure records are maintained of the user, the identifying information of the PCCD, and the length of the assignment.
9. Ensure approved encryption mechanism is installed and operational.
10. Provide locks and/or other security devices/methods intended to reasonably prevent the loss or theft of the device.
11. If the PCCD is intended for use outside the United States, other than the primary work location, seal the PCCD with the user's site DAA-approved tamper-indicating devices, prior to its removal from the primary work location.

B. Users, must:

1. Bear the responsibility for protection and integrity of NNSA data on PCCDs.
2. Prior to the receipt of an approved PCCD, agree to a usage policy and sign the user agreement.
3. Keep the PCCD password controlled, and allow no other person access to the password.

4. Connect the PCCD to the network, or otherwise arrange for routine servicing, no less than every 30 days for inventory and security software upgrades.
5. Abide by applicable prohibitions related to limited or exclusion areas, or the like.
6. Return the PCCD:
   a. on the agreed to date (if a temporary assignment);
   b. upon termination of employment (if a permanent assignment); or
   c. when no longer required (permanent or temporary assignment).
7. Ensure that the encryption mechanism installed on the PCCD is operational.
8. If using at a location outside the United States, other than the primary work location use the provided tamper-indicating devices.
9. In the event that classified information resides on a PCCD that is not specifically authorized to have this information, immediately make the notifications required in NAP-14.2-B.
10. If information is suspected of being compromised or of not being protected, the user will contact the system support help desk.
11. When taken from an NNSA site, an unattended PCCD must be secured in such a manner to reasonably prevent the loss or theft of the device. Users must utilize locks and other security devices/methods to secure PCCD when the device is unattended.

C. The NNSA CIO, Site Office Managers, and the Director of the Service Center, must ensure information technology support contractors have appropriate processes in place to implement these requirements.

V. REFERENCES

A. DOE CIO Guidance CS-9 Incident Management Guidance, dated January 2007

B. DOE CIO Guidance CS-12 Password Management, dated June 30, 2006

C. DOE O 203.1 Limited Personal Use of Government Office Equipment Including Information Technology, dated January 7, 2005

D. DOE O 580.1 Department of Energy Personal Property Management Program, dated December 7, 2005

E. DOE M 470.4-4, Information Security, dated August 26, 2005

F. NAP-14.2-B, NNSA Cyber Security Program, dated September 27, 2006

G. DOE O 3750.1, Workforce Discipline, dated August 21, 1992

H. 5 CFR, Administrative Personnel, Parts 731 and 752

I. US Code, Title 18, Crimes and Criminal Procedures

J. FIPS PUB 140-2, "Security Requirements for Cryptographic Modules," dated May 25, 2001

K. DOE M 251.1B, Departmental Directives Program Manual, dated August 16, 2006

VI. CONTACTS. Questions concerning this Policy should be directed to the NNSA Chief Information Officer at (202) 586-5617.

William C. Ostendorff
Principal Deputy Administrator

ATTACHMENTS

1. Definitions
2. NNSA User Agreement, "Explanation of Responsibilities and Applicable Penalties for Recipients of Portable Computing and Communication Devices (PCCD)"
3. Excerpts from NAP 14.2-B, Baseline Cyber Security Requirements

DEFINITIONS

1. *"External storage devices"* means any storage media, including but not limited to thumb drives, CDs, and memory cards), that may be attached to the PCCD.
2. "*Job assignment*" means the stated purpose and duties assigned to an NNSA staff member, in the performance of the position description.
3. "*Laptop computer*" means a personal computer (PC) designed to be portable and intended to facilitate the mobility of the user. Other popular names for such a device include "notebook computer."
4. "*Personal Digital Assistant (PDA)*" means any hand-held PCCD, such as, but not limited to, Blackberry brand devices and similarly equipped cellular telephones.
5. "*Portable Computing and Communications Device*" (PCCD) means any portable electronic device that stores NNSA data and has the capacity to: a) be used off site; b) access NNSA data while off site; or c) connect to NNSA networks while off site. Such devices include, but are not limited to laptop computers and PDAs. This definition does not include external storage devices or desktop computers.
6. *"Position description*" means the stated purpose, accountabilities, and essential/marginal duties for which an NNSA staff member is assigned.
7. "*Requestor*" means an NNSA staff member who requests a PCCD.
8. "*Senior Manager*" means an individual that reports directly to the NNSA Administrator, a Deputy Administrator, or an Associate Administrator. The responsibilities of a senior manager cannot be delegated.
9. "*Sensitive Unclassified Information*" includes but is not limited to: Personally Identifiable Information (PII), Privacy Act, Procurement, Financial, Unclassified Control Nuclear Information (UCNI), and Official Use Only (OUO).
10. "*Statement of duties*" means the same as "position description."
11. "*User*" means an NNSA staff member who is assigned a PCCD.

NNSA USER AGREEMENT

EXPLANATION OF RESPONSIBILITIES AND APPLICABLE PENALTIES FOR RECIPIENTS OF PORTABLE COMPUTING AND COMMUNICATION DEVICES (PCCD)

As a recipient of a PCCD, I am accountable at all times for the whereabouts and the safety of this device and its associated removable storage media.

I am obligated to protect and conserve this device and its associated removable storage media. I may use this device only for authorized purposes, as defined in 5 C.F.R. § 2635.704(b)(2), except to the extent that limited personal use is permissible under DOE O. 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology.* I may not allow anyone else to use it, except for official NNSA business, and with the understanding that I remain personally responsible for the device while it is being temporarily used by another individual associated with DOE.

I must at all times protect the storage and transmittal of the following categories of information: Personally Identifiable Information (PII), Privacy Act, Procurement, Financial, Unclassified Control Nuclear Information (UCNI), and Official Use Only (OUO). I understand that classified material cannot be placed on this device. In the event I suspect that the information on the device is not appropriately protected, I will contact my system support Help Desk.

Any suspected compromise of PII must be reported immediately to the responsible supervisor and the NNSA's Information Assurance Response Center (IARC). DOE policy requires all such incidents, suspected or confirmed, be reported within 35 minutes to the **IARC Hotline at (702) 942-2611 or iarc@iarc.nv.gov**.

I understand that the loss or theft of this device must be reported immediately by me to: (1) my system support Help Desk; (2) my responsible supervisor; (3) local law enforcement authorities; and (4) my property management officer as soon as I become aware of such loss or theft. I understand that I must obtain a report number from local law enforcement. If I suspect that this device or its associated removable storage media have been tampered with, I must immediately report this suspicion to my system support Help Desk.

The sale or conversion to my own personal use of this device is prohibited by 18 U.S.C. § 641 and may lead to imprisonment or a fine. I understand that this prohibition is not intended to forbid my limited personal use of the device as permitted under DOE Order 203.1.

I understand that I must connect the PCCD to the network, or otherwise arrange for routine servicing, no less than every 30 days.

I understand that failure to take appropriate steps to safeguard this device and its associated removable storage media; the deliberate or negligent destruction, loss or damage to this device; or my failure to fulfill any of the other responsibilities set forth above may result in administrative action including removal or suspension without pay from my position, pursuant to 5 C.F.R. § 731.201 Subpart B and 5 C.F.R. Part 752.

I have carefully read, and fully understand, my responsibilities as the recipient of this device, and the penalties for failure to carry out any of those responsibilities. A copy of the property receipt, with this signed attachment, will be provided for my records.

_____	_____
Signature	Print Name
_____	_____
Date	DOE Tag Number

Excerpts from NAP 14.2-B, Baseline Cyber Security Requirements

CHAPTER II

PERSONAL ELECTRONIC DEVICES AND PORTABLE COMPUTERS

1. INTRODUCTION. Establish requirements for the use of personally owned or government owned Personal Electronic Devices (PEDs) and portable computers, hereafter called portable computing devices, in the National Nuclear Security Administration (NNSA) and all organizations under its cognizance. These requirements apply to any portable computing device (see definition in Attachment 4) that collects, stores, transmits, or processes unclassified or classified NNSA information or is located in any security area (Property Protection Area (PPA), Limited Area (LA), Exclusion Area (EA), or Protected Area (PA)) where NNSA information systems are used.
2. REQUIREMENTS.
   a. Visitors to any NNSA Property Protection, Limited, Exclusion, or Protected Area must be advised, prior to entry, of the requirements of this policy.
   b. **Personally owned** portable computing devices:
      (1) Are prohibited from use within any NNSA Property Protection, Limited, Exclusion, or Protected Area;
      (2) May be used within an NNSA Property Protection Area only in accordance with the procedures defined in the NNSA element's Cyber Security Program Plan (CSPP);
      (3) Are prohibited from any connection, i.e., assigned a network address, to any NNSA or NNSA-contractor local area network, wide area network, or information system component, except as described in the NNSA element's CSPP;
      (4) Are prohibited from storing, processing, receiving, or transmitting classified information; and
      (5) May be used to store, process, receive, or transmit unclassified information with a confidentiality Consequence of Loss of "Medium" or less only in accordance with the policies and procedures defined in the NNSA element's CSPP.
   c. **US government owned** portable computing devices with radio frequency (RF) or Infra-red (IR) capability (e.g. Wireless Information System (W-IS) may be used in NNSA Property Protection, Limited, Exclusion, and Protected Areas where sensitive unclassified or classified information is processed, stored, transferred, or accessed on information systems, or where sensitive unclassified or classified information is discussed or displayed via electronic methods after completion of a risk assessment of the specific intended use and only if the portable computing device:
      (1) Authenticates all users in accordance with the process described in an approved System Security Plan;
      (2) Employs up-to-date malicious code detection software;
      (3) Applies National Security Agency (NSA)-approved type 1 encryption on all communications to and from the portable computing device involving classified information;

(4) Comply with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements;

(5) Comply with NNSA PCSP requirements;

(6) Configured with preferences and settings for services approved by the cognizant DAA;

(7) Configuration managed and controlled; and

(8) Applies DOE approved encryption algorithms on all communications involving sensitive unclassified information.

d. All portable computing devices with an audio recording capability are used in NNSA Property Protection, Limited, Exclusion, or Protected Areas in accordance with NNSA TEMPEST and TSCM policies and the NNSA element's CSPP.

e. The administrative and physical controls, including TEMPEST, used to reduce the risks from the use of any portable computing devices must be documented in the element's CSPP.

f. Site personnel must be trained on the rules of use for portable computing devices that are allowed on NNSA sites. This training must be documented.

g. Supervisory personnel for an individual (Federal or contractor) must be notified of any violation of NNSA policies or element portable computing device procedures. The responsible supervisory personnel must take disciplinary action in accordance with the NNSA element's personnel performance evaluation system.

h. Portable computing devices used at a location, outside the United States, other than the assigned user's primary work location – ("home" site of the user) must be sealed with NNSA-approved tamper-indicating devices prior to removal of the portable computing device from the "home" site. The tamper-indicating devices must be placed to allow normal use (i.e., removal and insertion of components such as removable hard drives and batteries). The hardware and software technical review process for all portable computing devices must be documented in the element's CSPP. The cognizant Designated Approving Authority (DAA) may approve alternative protection measures when the use of tamper-indicating devices are ineffective or because of operational requirements.

i. If portable computing devices are operated as desktop units (i.e., they do not leave the user's primary work location / "home" site), they are to be operated in accordance with the System Security Plan for the information system.

j. Visitors bringing a portable computing device into a Property Protection, Limited, Exclusion, or Protected Area may be required to meet additional requirements or entry of the portable computing device will be denied.

k. Portable computing devices or components of portable computing devices, such as removable disk or disk drives, containing classified information must be protected and transported in accordance with Classified Matter Protection and Control requirements.

l. Portable computing devices or components of portable computing devices, such as removable disk drives, containing information in the Unclassified Protected or Unclassified Mandatory Protection information groups, as defined in Attachment 3, NAP-14.1, *NNSA Cyber Security Program,* must be protected and transported in accordance with protection requirements for the sensitive information they contain.