PII SPOT CHECK DOCUMENTATION

This checklist is an internal document and is to be used by command leadership to assess the level of compliance in the handling of Personally Identifiable Information (PII) as delineated by law and/or by other applicable DoD/DON policy guidance. Department of the Navy activities are required to conduct two PII spot check cycles per year (Normally during June & December). NSWCDD is required to consolidate spot check results and improvement actions and report them to NAVSEA.

> **Personally Identifiable Information (PII) Definition** - OMB defines PII as: Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as his or her name, SSN, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

General Instructions:

- If you encounter unattended PII as you conduct your spot-check, DO NOT leave the PII document(s) unattended. Provide the PII document(s) to the Manager/Supervisor of the Organizational Unit responsible to control PII access.
- It is important to note that most business-related PII (titles, work phone numbers, work email addresses, office codes) when lost, stolen or compromised, and, not associated with other traceable personal information, is not cause for submission of a PII breach report; therefore, please do not report these instances as a "compromise" for purposes of completing this spot-check.
- Always describe what was found (e.g., Document #1 contained home phone numbers of employees in our office. Document#2 contained SSN's of three individuals. Document #3 contained birth date of our support contractor…) and what action was taken.
- **Fill the name and contact information of those conducting the spot check on each page. DO NOT include any other names in the spot check documentation.**
- Please forward the completed documentation to the NSWCDD Privacy Act Coordinator via your Department's Senior Management.
- The NSWCDD Privacy Act Oversight Committee will develop process improvement plans for all systemic/process findings.
- **If a PII Breach is identified, please report it within one hour to your supervisory chain and to the NSWCDD Privacy Act Coordinator.**

For additional guidance and information, go to the NSWCDD Privacy Program website located in the NSWCDD Information Tool https://wwwdd.nmci.navy.mil/cgi-bin/wcit.pl , refer to the NSWCDD Users Guide to PII and/or contact NSWCDD's Privacy Act Coordinator.

(Privacy Act Coordinator) **Work Phone:**
(Alternate) **Work Phone:**
Privacy Program Email:

This Spot Check document is an auditable record and should be kept on file for three years.

COMMAND LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check:		Activity:	
Performed by:		Title:	**Privacy Act Coordinator**
Phone:		Email:	

Activity Privacy Act Coordinator information, if different than above.

Name __________________ Phone: ______________ Email:_______________________

Activity Alternate (if applicable)

Name: Phone: Email:

A. ADMINISTRATIVE

1. The command has an implementing Privacy Act instruction. Reference: SECNAVINST 5211.5E 7.h. (7) - pg. 13

Yes (NSWCDDINST 5211.1C) (Latest Instruction NSWCDDINST 5211.1D Expected By 1 March 2011.)

2. The command Privacy Act Coordinator has been identified in writing with clear roles and responsibilities identified. Reference: SECNAVINST 5211.5E 7.h -- pg. 13 **Yes**

3. DON CIO message 301540Z Nov 06 Breach reporting policy provides the following reporting policy. Privacy Officer is notified within one hour of loss or suspected loss and affected personnel have been contacted as quickly as possible but in no less than 10 days from discovery of PII loss.

a. Was your activity informed of the DON reporting policy? **Yes**

b. Number of reported incidents for __**1**_ FY09 & _**9**__FY10 & _**1**_FY 11

c. Was notification made to the affected members of the breach(s) within 10 days? **Yes**

Action Taken:
d. If you answered “No” to 13a above, describe action taken to inform:
____

4. Has the command disseminated guidance to its personnel on how to properly mark email, messages, letters, etc., that contain PII prior to transmission? Reference: SECNAVINST 5211.5E 7.i.(5) – pg. 15 “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE.”.

Yes (Included in: Annual Mandatory PII Training, NSWCDDINST 5211.1C, and in the NSWCDD Users Guide to PII)

5. Has the command taken action to eliminate or reduce the need for the use of SSN’s? Reference: SECNAVINST 5211.5E 9.C.(6) – pg. 22

Yes (review of local requirements)

COMMAND LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: _______________ Activity: **NSWCDD Dahlgren Site**
Performed by:

6. Consult your activity's **Forms Manager** to determine if a process is in place to review forms that collect PII from individuals to ensure that all collections are authorized and that the forms contain Privacy Act Statements.

a. Does your activity have a process in place to review forms that collect PII directly from individuals? **Yes (There is a formal procedure for all NSWCDD forms)**

Action Taken:
b. If you answered "No" to 5a above, describe action taken to ensure compliance:
____

B. INFORMATION SYSTEMS

1. For DITPR DON registered systems that contain PII for DON personnel and the public, has there been a PIA submitted to the DON CIO office for approval? **Reference: SECNAVINST 5211.5E 7.e.(1) – pg. 12**

a. Number of systems requiring PIA's ____
b. Number of systems with PIA's submitted _____

2. Does the organization have protocols established to ensure PII is not inadvertently posted on a public or restricted access website? **Reference: SECNAVINST 5211.5E 7.d.(8) – pg. 11**

Yes

C. TRAINING.

1. Consult your activities Training Coordinator to ensure that all PII training certificates are on file and review procedures for newly assigned personnel to receive training during orientation.

a. Does your activity Training Coordinator have copies of the FY09/FY10 PII training certificates on file, including applicable contractors? **No**

b. If copies are not with training coordinator, who maintains these auditable certificates:
Department Training Coordinators

c. What process is in place to ensure new hires take the PII training:
Employees are informed of mandatory training requirements during the in-brief/ initial orientation process.

Action Taken:
d. If copies could not be located, describe action taken to ensure compliance:
____

COMMAND LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: ________________ Activity: **NSWCDD Dahlgren Site**
Performed by:

NOTES:

ORGANIZATIONAL UNIT LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: ________________ Organizational Unit: ________________
Performed by: ________________ Phone: ________________
Email: ________________

A. PAPER RECORDS

1. Spot-check copiers and network printers located in common areas within your Organizational Unit for documents containing PII.

a. Number of Copiers checked: ____
b. Number of Copiers where PII was found: ____
c. Number of Printers checked: ____
d. Number of Printers where PII was found: ____
e. Describe what was found: (**Note: Describe what was found: e.g., Document #1 contained home phone numbers of employees in our office. Document#2 contained SSN's of three individuals. Document #3 contained birth dates of our support contractors…*)
____
____

Action Taken:
f. If PII was found, describe what action was taken, if known:
____

2. Spot check all Fax machines located in common areas within your activity for documents containing PII.

a. Number of fax machines checked: _____
b. Number of fax machines where PII was found: ____
c. Describe what was found: (* see note above) ______________________________________
____

Action Taken:
d. If PII was found, describe what action was taken, if known:
____

4. Spot check a sampling of recycle containers at your activity for recognizable PII. (C*heck 1 container if the organizational unit has 5 or less. Check 2 if the organizational unit has 6 to 10 containers. Check 3 if the organizational unit has 11 to 30. Check 10% if the organizational unit has over 30 containers.)* Reference: SECNAVINST 5211.5E 8.b.(1) through (3) – pg. 19

a. Number of containers checked: ____
b. Number of containers containing PII: ____
c. Describe what was found: (*see note above)______________________________________
____

Action Taken:
d. If PII was found, describe what action was taken, if known:
____

ORGANIZATIONAL UNIT PII SPOT CHECK DOCUMENTATION

Date of Spot check: _______________ Organizational Unit: _______________
Performed by: _______________

5. At random, spot check 10 % of burn bags within your organizational unit to ensure that if they contain PII that they are secure from unauthorized access by individuals who do not have a need to know. Reference: SECNAVINST 5211.5E 8.b.(1) through (3) – pg. 19

a. N/A ____ Number of bags checked ____
b. Number of bags containing PII and not secured ____

Action Taken:
c. If PII was found, describe what action was taken, if known:
____

6. Check bulletin boards in your organizational unit's work spaces, Kitchenettes and Copy Rooms to ensure that no "third party" PII information is posted. *(Look for lists of birthdays, personal cell phone numbers, home addresses and home phone numbers. Not interested in self postings, i.e. selling of cars, rentals)*

a. Number of boards checked: ____
b. Number of "third party" PII found: ___
c. Describe what was found: (*see note above)______________________________________
____

Action Taken:
d. If PII was found, describe what action was taken, if known:
____

B. ELECTRONIC RECORDS/HARDWARE. (Likely to contain PII)

1. Spot-check "Intranet/Internal" sites/applications for PII that is available to individuals who do not have a need to know. **Reference: SECNAVINST 5211.5E 18.D.(6) – pg. 47**

a. Number of sites/applications checked: ____
b. Number of records with PII: ____

Action Taken:
c. If PII was found, describe what action was taken, if known:____________
____

2. Naval Message DTG 171952Z APR 07 "Safeguarding personally Identifiable Information" requires that any laptop, mobile computing device or removable storage media that contains PII on 25 or more individuals on a single device be restricted to DoD workplaces. When compelling operational needs require removal, the device(s) must be handled as follows: 1) signed in and out, 2) configured to require certificate-based authentication, 3) set to implement screen lock and 4) all PII will be encrypted. **Storage of any form of PII on "personally" owned laptops, mobile devices, and removable storage is prohibited as of 1 October 2007.**

ORGANIZATIONAL UNIT PII SPOT CHECK DOCUMENTATION

Date of Spot check: ________________ Organizational Unit: ________________
Performed by: ________________

Identify all portable equipment (to include but not limited to laptops, mini external drives, USB drives, and external hard drives) which contain data on 25 individuals or more, in your activity.

a. Does your activity have a check in/out log for portable equipment containing PII on over 25 individuals? **Expectation of approval of NSWCDDINST 5211.1D, with Check Out/In Form as a Reference, 1 March 2011.**
b. If yes to 1a above, is your activity using the check in/check out log? by **1 March 2011**
c. If no to 1a, what other check in/check out practice is being used?
____

Action Taken:
c. If no check in/out practice is in place, describe what action was taken, if known:
____

3. For Non-NMCI networks: Data at Rest (DAR) on laptops, desktops and removable storage media should be protected.

a. Is your organizational unit currently using "Mobile Armor" to protect DAR on Non-NMCI laptops, desktops and removable storage media? **Yes / No**
b. If no, is your activity currently using software to protect DAR? **Yes / No**
c. If so, what software is in use? ________________________________
d. If no software is in use, by what means are you protecting sensitive data?
____

Action Taken:
e. If not in compliance, describe what action was taken, if known:
____

4. For NMCI networks: organizational units are required to use “GuardianEdge” to protect Data at Rest (DAR) on laptops, desktops and removable storage media.

a. Is your activity currently using “GuardianEdge” to protect DAR on NMCI laptops, desktops and removable storage media? **Yes / No**

Action Taken:
b. If not in compliance, describe what action was taken, if known:
____

NOTES:

EMPLOYEE/CONTRACTOR LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: ________________ Organizational Unit: ________________
Performed by: ________________ Phone: ________________
Email: ________________

1. Does the organizational unit ensure PII is only accessible to authorized personnel, is not left unattended and is stored in an appropriate secured/locked space, cabinet, file, etc. when not in use and after normal working hours?

a. PII stored in secured/locked workstations/offices? **Yes____ / No _____**
b. PII stored in secured/locked cabinet, file, drawer, etc.? **Yes____ / No _____**
c. Describe what was found: ____
____

Action Taken:
d. Describe what action was taken, if known:
____

2. Is PII training documentation/certification available for review? a. **Yes____ / No _____**

Action Taken:
b. Describe what action was taken, if known:
____

3. At random, spot check laptops/portable devices. Select up to 10 documents (Word, Excel, etc.) likely to contain PII, for proper password protection or encryption. *(Include supervisors, Admin Officers and others likely to have PII data. If you are able to access without a password - close documents as soon as you identify PII data. Do not read contents of documents)*

a. Number of Portable Equipment checked: _______
b. Number of documents with PII not protected: _______
c. Describe what was found: (*see note above)____
____

Action Taken:
d. If un-protected PII was found describe what action was, if known:
____

3. Spot check PDA/Blackberries to ensure time out function is enabled and unit is password protected.

a. Does your organizational unit have PDA/Blackberries? **Yes / No**
b. Number of units checked: _____
c. Number of units without time-out function and without password protection: _________

Action Taken:
d. If un-protected describe what action was taken, if known:
____

EMPLOYEE/CONTRACTOR LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: _______________ Organizational Unit: _______________
Performed by: _______________

4. Spot check your organizational unit Shared Drives for “un-locked/un-encrypted/unprotected” files, which are likely to contain PII.

a. Does your activity use shared drives? **Yes / No**
b. Number of shared files checked: ____
c. Number of shared files containing PII and not password protected: ____
d. Describe what was found: (*see note above)______________________________________
____

Action Taken:
e. If un-protected PII was found, describe what action was taken, if known:
____

5. Spot check up to 10 paper/electronic records, reports, and emails containing PII for appropriate markings.

a. Number of paper records checked ____
b. Number of paper records with appropriate marking ____
c. Number of reports checked ____
d. Number of reports with appropriate marking ____
e. Number of locally generated forms ____
f. Number of locally generated forms with an appropriate Privacy Act statement ____
g. Number of emails checked ______
h. Number of emails with appropriate markings ____

i. Describe what was found: (*see note above)___________________________________
____

Action Taken:
j. If un-marked PII was found, describe what action was taken, if known:
____

6. Records are to be kept in accordance with retention and disposal requirements set forth in SECNAVINST 5210.8D.

a. Is action taken at your organizational unit to ensure, on a routine basis, that records (paper and electronic) are disposed of in accordance with SECNAVINST 5210.8D? **Yes/No**

b. If yes, what is the practice: **(i.e. Clean up day; File destruction at the end of the fiscal year…)**
____

EMPLOYEE/CONTRACTOR LEVEL PII SPOT CHECK DOCUMENTATION

Date of Spot check: ________________ Organizational Unit: ________________
Performed by: ________________

NOTES: