PII SPOT CHECK FORM

This form is an internal document and will 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 specific DoD/DON policy guidance. Commands should tailor this form to fit their specific requirements. For additional guidance and information contact the Command Privacy Official at XXX-XXXX. This Spot Check form is an auditable record and shall be kept on file for three years by the Privacy Official. **Ref: ALNAV 070/07: SECNAV WASHINGTON DC 042232Z OCT 07.**

PII of concern is information which carries some risk-of-harm to an individual or to the command should the information be accessed by unauthorized personnel. PII of this nature is considered to be "sensitive" and must be protected. SENSITIVE PII includes but is not limited to: Social Security number (SSN), date and place of birth, personal financial information, personal medical information.

PII that is releasable to the public in accordance with law (5 USC §552) or regulation (5 CFR §293.311 or 32 CFR §310.22) or is commonly used in the work environment (OSD 15041-07) is not considered to be of risk to an individual nor to the command. PII of this nature is NOT "sensitive". All non-sensitive PII must be examined in its context of use. Context of use can make non-sensitive PII (a list of 'just names') sensitive if the list is contextually associated with sensitive information (list of 'just names' in a folder marked "Employees who failed a drug test").

The following PII is NORMALLY considered to be NOT SENSITIVE for all employees and contractors: name, work phone, work email, code, rank, work location, badge number, and assigned position.

ADMINISTRATIVE

1. Name of the individual assigned to conduct this spot check is _____

2. Area of responsibility checked (Bldg/Floor) _____ (Code) _____

3. Date spot check conducted _____

PAPER RECORDS

1. Has the command developed a PII records disposal program? _____

2. ____ Number of personnel onboard ____ Number of personnel that received PII training in last 12 months

Ref: GENADMIN: DON CIO WASHINGTON DC 181905Z DEC 08

3. ____ Number of PII breaches reported this calendar year ____ Number of personnel notified

4. Does the command have a SSN reduction plan in place? _____

5. Spot check 10 % of burn bags within your area of responsibility. Ensure that if they contain PII that they are secure from unauthorized access by individuals who do not have a need to know. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of bags checked ____ Number of bags containing PII and not secured ____

6. Spot check 10 % of recycle containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of containers checked ____ Number of containers containing PII ____

7. Spot check 10 % of waste containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of containers checked ____ Number of containers containing PII ____

8. For static bulletin boards disseminating/displaying command information, check for the presence of PII. PII should only be available to individuals with a need to know. **Ref: SECNAVINST 5211.5E 18.d. (6) – pg. 47**

Number of boards checked ____ Number of examples of where PII was found ___

ELECTRONIC RECORDS/HARDWARE

9. For Non-NMCI networks: Is your activity currently using "Mobile Armor" to protect DAR on non-NMCI laptops, desktops and removable storage media? If no, when will a DAR product be implemented? If using other than Mobile Armor, provide date that a DON CIO waiver was granted? _____

10. For NMCI networks: Have you verified with your IAM that the data at rest encryption solution has been pushed to all NMCI laptops and desktops? (Note: laptops must be plugged in to the NMCI network to receive the push) _____

Ref: GENADMIN: DON CIO WASHINGTON DC 091256Z OCT 07

11. Has a check in /check out log for all laptops and portable electronic equipment been created and implemented for all such devices that contain PII on >24 individuals and that are transported outside a secure government space. Does the supervisor maintain this log and can it be produced upon request. **Ref: DONCIO 171952Z APR 07**
_____

12. Spot check at least 10% of PDA/Blackberries within your area of responsibility. Ensure the time out function is enabled and each unit is password protected. **Ref: SECNAVINST 5211.5E 18.d. (5) – pg. 47**

Number of units not in compliance ____ Not applicable, AOR has no PDA's _____

13. Spot check 10% of laptops within your area of responsibility. Ensure all data is encrypted, the time out function is enabled and each unit is password protected. **Ref: SECNAVINST 5211.5E 18.d. (5) – pg. 47**

Number of laptops checked ____ Number of laptops not configured as required _____

14. Search and spot check 25% of files on the shared drives within your area of responsibility. Ensure that no PII has been posted.

Number of files checked ____ Number of files containing PII ____

15. Are all computer hard drives physically destroyed when sent to disposal? _____

16. Are copier/printer machine hard drives sanitized or destroyed prior to disposal? _____

WEBSITES

17. Spot check 25% of AOR web sites (internal and external), searching for PII that is available to individuals who do not have a need to know. **Reference: SECNAVINST 5720.47B 7.d. (1) – pg. 4**

Number of sites checked ____ Number of records with PII ____ N/A, no AOR web site _____