PII Compliance Spot Check Example

1. Command Oversight: Does the command/organization provide oversight to lower echelon commands? How many commands? What are the names? Who are the POCs? How do you maintain oversight? List examples.

2. If you have questions about PII or Privacy, who do you contact? What is a good website for one stop "shopiing" for DON PII?

3. Does the command have a Privacy Act Coordinator, PII Coordinator or Privacy Officer designated in writing? Who has been designated? Provide a copy of the designation letter. What is the date of the Privacy Officer/PII Coordinator Designation letter? How long have they been designated? (This is required for Echelon II and III. Below Echelon III require breach reporting POCs.)

4. Does the command have a PA Team? Who is represented?

5. Have all command members (military, civilians and contractors) completed the annual privacy training by August 31, with newly reporting members completing the training upon arrival (or showing proof of completion within 12 months from a previous command)? (Responsibility: Commanders, Commanding Officers, Officers-in-Charge.)

6. Does the command's CO or OIC conduct semi-annual spot checks, utilizing the spot check form? Are discrepancies corrected? (This is required for all DON commands.) [retain for three years]

Specifically: Commanders/Commanding Officers/Officers-in-charge will ensure that supervisors conduct a spot check of their assigned areas of responsibility, focusing on those areas that deal with PII on a regular basis. Spot checks will be conducted on a semi-annual basis. Auditable records will be maintained by the command privacy act coordinator or other designated official. Corrective action should be taken immediately where weaknesses are identified.

7. Have there been any reported breaches in the last 12 months? Has corrective training been conducted? Breach reports should be maintained for two years. Are the records available for review?

8. Are all command e-mails containing PII (or FOUO) information encrypted and contain the classification marking? "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

9. Are all command records containing PII properly labeled? Specifically "Mark all documents that contain PII (e.g., letters, memos, emails, messages, documents faxed, etc) FOUO. Consider using a header/footer that reads: "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

10. Are bulletin boards and individual workspaces clear from inadvertent disclosure of PII?
Specifically: "Ensure that PII is not left out in the open or circulated to individuals not having an official need to know."

11. Do all command routed folders, containing Privacy Information, utilize the Privacy Cover Sheet, DD Form 2923, Mar 2009 (attached), or a command generated cover sheet? (Best Practice). (

12. Has the command designated a command POC (can be the same as the Privacy Act Officer/PII Coordinator), to report breaches and have written breach procedures been created? Request a copy of the written breach procedures.

13. Is the command actively engaged in reducing SSN use (DON SSN Reduction Plan, Phases 1, 2, and 2)? Who is the Command Forms Manager? Has a review been conducted of all, official forms, unofficial forms, spreadsheets, rosters, electronic collections, etc., to locate collections of the SSN and where found, provide justification for continued use or elimination/substitution (using DoD ID)? Is the FAX machine being used to transmit the SSN?

PII Compliance Spot Check Example

14. Does the command publish POD or POW notes on good practices for protecting PII (see the DON CIO site for ideas)?

15. Does the command have a PII or Privacy Instruction (REQUIRED for Echelon II and Echelon III)? Are breach procedures included?

16. Does the command utilize recycle bins? Are they clearly labeled for FOUO (locked bins) or unclassified material if unlocked?

17. Has the command created the appropriate electronic permissions on command shared drives SharePoint portals to ensure access on a need to know basis only?

18. Does the command utilize/display PII signs available on the DON's Privacy website?

19. Does the command have any Privacy Impact Assessments (PIAs)? If so, request copies. Are they current?

20. Review the command website to ensure no PII is posted.

21. Is PII only collected (minimized) to support a DON function or program as authorized by law?

22. Are Privacy Records/PII properly destroyed? Specifically:

(1) Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) DON activities may recycle PA data. Such recycling must be accomplished to ensure that PII is not compromised. Accordingly, the transfer of large volumes of records in bulk to an authorized disposal activity is not considered a disclosure of records.

(3) When disposing of or destroying large quantities of records from a system of records, DON activities must ensure that the records are disposed of to preclude easy identification of specific records.