Compliance

- Annual PII training must be completed by new employees within 30 days of reporting onboard.
- Annual PII training must be completed by existing employees by 31 Aug. Not more than one year should elapse between each training completion.
- All DON personnel, including contractors, must complete annual PII training. Commands must maintain auditable certificates of completion.
- The mandatory PII training course for Navy and Marine Corps is available on NKO, TWMS, and MarineNet.
- Refresher training is available; it is recommended for DON personnel who mishandle PII.
- All offices that handle PII must complete a Compliance Spot Check twice yearly. Commands must maintain auditable records.

Social Media

- Assume all information shared on social media sites could be made public.
- Do not post or discuss work related information, especially sensitive/classified information.
- Use privacy settings and controls when possible to limit access to your information.

Breach Reporting

- Contact your privacy coordinator or supervisor as soon as you suspect or have an actual loss or compromise of PII.
- Report PII breaches within one hour of discovery to US-CERT and your chain of command in accordance with DON CIO or Marine Corps guidance.
- Upon receipt of a PII Breach Report, the DON CIO or HQMC C4 will provide the reporting command with further direction.

Mailing PII

- Document should be marked "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- It is considered a best practice to double wrap the document and mark the inner wrapper.
- Another best practice is to use DD Form 2923 "Privacy Act Data Cover Sheet" as appropriate.
- A document containing PII should be mailed to only those with an official need to know.
- Use a mailing service that can provide tracking information; this is also a best practice.

FOR MORE INFORMATION

Secretariat and Navy personnel contact the DON CIO Privacy Team
E-mail: don.privacy.fct@navy.mil
Visit the Web at: http://www.doncio.navy.mil/privacy

Marine Corps personnel contact IA C4 HQMC
E-mail: hqmc_c4cy_idmgt@usmc.mil
Visit the Web at: https://c4.hqi.usmc.mil/pii.asp
Ask an Expert: http://www.doncio.navy.mil/askanexpert.aspx

April 2013

Department of the Navy
Users Guide to PII

PERSONALLY IDENTIFIABLE INFORMATION

Department of the Navy
Chief Information Officer

1000 Navy Pentagon
Washington, DC 20350-1000

Protective Measures

Definition of PII

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity. Examples include but are not limited to: name, social security number (SSN), date of birth, home address, home phone number, personal e-mail address, financial information, fingerprints, photograph, and medical information.

Collecting PII

If you collect, maintain or use PII, it must be required to support a DON function or program as authorized by law, Executive Order or operational necessity. Whether you are working from your desk at the office, on a government furnished device at home, at sea, or in the field, it is your responsibility to:

- Ensure that the information entrusted to you in the course of your work is secure and protected. PII must only be accessible to those with an "official need to know".
- Minimize the use, display or storage of SSNs and all other PII. The DoD ID number or other unique identifier should be used in place of the SSN whenever possible.
- Keep the information timely, accurate and relevant to the purpose for which it was collected.
- Delete personal information when no longer required and remember to follow SECNAV M-5210.1, the DON Records Management Manual, regarding retention and disposition requirements.
- Immediately notify your supervisor if you suspect or discover that PII has been lost or compromised.

Policy References:

DON Privacy Program: SECNAVINST 5211.5 (Series) and as follows:
SSN Reduction: DON CIO Washington DC 192101Z JUL 10 and DON CIO Washington DC 171625Z FEB 12
E-mail: DON CIO WASHINGTON DC 032009Z OCT 08 and SECNAVINST 5211.5 (series))
FAXing: DON CIO WASHINGTON DC 081745Z NOV 12
Scanning: DON CIO WASHINGTON DC 171625Z Feb 12 and DON CIO WASHINGTON DC 081745Z NOV 12
Electronic Storage Media: DON CIO WASHINGTON DC 281759Z AUG 12
Network Shared Drives: DON CIO 201839Z NOV 08
Training and Compliance: ALNAV 07/07 and DON CIO WASHINGTON DC 181905Z DEC 08
DON Breach Reporting: DON CIO 291652Z FEB 08

SSN Reduction

- Limit the use of the SSN in any form (including the last four digits); substitute the DoD ID number or other unique identifier whenever possible.
- Collection of the SSN must meet one of the acceptable use criteria and be formally justified in writing.
- Never include the SSN in a personnel roster.
- Use only officially issued forms (i.e., those that have a DoD, DON, or other government number). Those that collect PII should also have a Privacy Act Statement (PAS).
- Never post SSNs on public facing websites.

IT Equipment

- Never leave your laptop unattended.
- Keep your laptop in a secure government space or under lock and key when not in use.
- Laptops and mobile electronic equipment must have full disk /data at rest (DAR) encryption (must be a DoD/DON approved DAR solution).
- Mark all external drives or mobile media with "FOUO, Privacy Sensitive."
- Never store PII on personal electronic storage devices.
- Do not maintain PII on a public Web site or electronic bulletin board.

E-mail

- E-mail containing PII must be digitally signed and encrypted.
- Marine Corps policy requires "FOUO Privacy Sensitive" in the subject line of emails containing PII. The Navy considers this a best practice.
- Ensure the body of the e-mail containing PII includes the following warning: "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- Ensure you are sending the email to the correct recipients and all have an official need to know.
- Ensure you know what your attachment contains (i.e., PII) prior to sending. Check all tabs if the attachment is an EXCEL spreadsheet.
- Phishing continues to be on the rise. Ensure you only open and respond to legitimate e-mails.

Printed Materials

- Verify printer location prior to printing a document containing PII.
- Ensure all printed documents with PII are properly marked with "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- As a best practice, transport/hand carry PII documents in a double wrapped container/envelope and use a "Privacy Act Cover Sheet" (DD FORM 2923) as a cover.
- Safeguard all documents when not in your direct possession by prohibiting access by those without an official need to know.

Faxing

- FAXing PII is prohibited except:
  - When another more secure means is not practical.
  - When a non-DON process requires faxing.
  - When required by operational necessity.
  - When faxing Internal Government Operations PII (i.e., office phone, office email, badge number).
- As a best practice, use a "Privacy Act Cover Sheet" (DD FORM 2923) as a cover.
- Verify receipt by the correct recipient.
- External customers should be encouraged to use the US Postal Service or another secure means (i.e., encrypted emails or Safe Access File Exchange (SAFE)).

Scanning

- Scanned documents shall be transmitted using a secure means (i.e., encrypted emails or SAFE).
- The following scanning restrictions apply to network attached multifunction devices (MFDs) and scanners (not to MFDs or scanners connected directly to a user's workstation).
  - "Scan to email" may be used only if the sender can verify that the intended recipients are authorized to access the scanned file and that the email containing the scanned file is sent encrypted.
  - "Scan to file" or "scan to network share" may be used only if the sender can verify that all users are authorized to have access to the scanned file or network share location.

Electronic Storage Media

Internal and removable electronic storage media include, but are not limited to: laptops, printers, copiers, scanners, MFDs, hand held devices, CDs/DVDs, removable and external hard drives, and flash based storage media.

- Classified electronic storage devices must be physically destroyed.
- Unclassified Naval Criminal Investigative Service (NCIS) and Navy Nuclear Propulsion Information (NNPI) electronic storage media must be physically destroyed.
- Except as noted above, unclassified electronic storage media must be destroyed unless a waiver has been requested and approved IAW DON CIO WASHINGTON DC 281759Z AUG 2012.

Network Shared Drives

- For files/folders containing PII, ensure that controls are in place restricting access to only those with an official need to know.
- Limit storage of PII on shared drives whenever possible.
- Delete files containing PII in accordance with SECNAV M-5210.1, the SECNAV Records Management Manual.
- Verify that access controls/permissions are properly restored following maintenance.

Disposal

- Records should be rendered unrecognizable or beyond reconstruction.
- Do not discard documents containing PII in trash or recycle bins.

Shredding

- As a best practice use a cross cut shredder.
- Residue size: As a best practice refer to NIST Special Publication 800-88.
- An alternative is to contract with a GSA approved shredder service.
- Using burn bags is another good option.