

Social Media

- Do not post PII on social media sites.
- 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.

Compliance

- Initial PII awareness training for all new DON employees (military, civilian and contractors (if required in the contract)) must be completed prior to the employee being granted network access or within 30 days of reporting.
- Employees (military, civilian and contractors (if required in the contract)) must complete annual PII training by 30 September. Not more than one year should elapse between each training completion.
- Commands must maintain auditable records of training completions.
- The DON annual PII training course for Navy and Marine Corps is available on Navy eLearning (NKO), TWMS, and MarineNet.
- All offices that handle PII must complete a Compliance Spot Check twice yearly. Commands must maintain auditable records of spot check completions.
- Ensure all applicable Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) privacy clauses are included in DON contracts where contractors manage or have access to PII.
- The collection of PII may require a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA). Check with your privacy official for guidance.

Breach Reporting

- Contact your privacy coordinator or supervisor as soon as you suspect or have an actual loss or compromise of PII.
- Report all suspected or confirmed PII breaches within one hour of discovery to your chain of command.
- In accordance with DON guidance use SECNAV Form 5211/1 to report suspected or confirmed breaches.
- Upon receipt of a PII Breach Report, the DON CIO or HQMC C4 will provide the reporting command with further direction.
- Submit SECNAV Form 5211/2 to complete after action reporting and close the breach.

Mailing PII

- When mailing 25 or more hard copy records containing PII, the package shall be double wrapped and the inner package marked "For Official Use Only - Privacy Sensitive. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- DD Form 2923 (SEP 2010) Privacy Act Data Cover Sheet must be inserted inside the outer wrapping.
- All such packages must be tracked with government or commercial delivery services.
- Documents containing PII should be mailed to only those with an official need to know.

FOR MORE INFORMATION

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

Marine Corps personnel contact
DC/I C4 Cybersecurity (CY) Division at:
E-mail: hqmc_c4cy_idmgt@usmc.mil

Questions and/or comments?
Contact the DON Privacy Team at:
<http://www.doncio.navy.mil/askanexpert.aspx>



Department of the Navy

User's Guide to

PERSONALLY IDENTIFIABLE INFORMATION (PII)



FULL NAME
AGE GENDER
TELEPHONE NUMBER
TAX INFO ADDRESS
CITIZENSHIP
BIRTH DATE EDUCATION
TRAVEL DOCUMENT
NATIONAL IDENTITY NUMBER
CRIMINAL RECORD
NATIONALITY
MARITAL STATUS
INCOME INFO
IDENTITY DOCUMENT
BANK ACCOUNT NUMBER
OCCUPATION VISA INFO
MEDICAL RECORD

Protective Measures

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 using the SECNAV Form 5213/1.
- Never include the SSN in rosters, questionnaires, or surveys.
- Never post SSNs on public facing websites.



- Never use any part of the SSN as part of the naming convention when saving electronic files.

IT Equipment

- Never leave your laptop unattended.
- Keep your laptop in a secure space when not in use.
- Laptops and mobile electronic equipment, including CDs, must have DoD/DON approved full disk /data at rest (DAR) encryption.
- Mark all external drives, CDs, and other mobile media that store PII with "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties." Include date and contact information for individual creating and encrypting the media. For CDs, consider using the CD PII label available on the DON privacy web site.
- Storage of PII on personal electronic storage devices is not allowed.
- Do not maintain PII on a public website 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 e-mails containing PII. The Navy considers this a best practice.
- Ensure the body of an e-mail containing PII includes the following warning: "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."
- Confirm you are sending the e-mail to the correct recipients and all have an official need to know. Ensure the e-mail remains within the .mil domain.
- Know what your attachment contains (i.e., PII) prior to sending. Check all tabs if the attachment is a spreadsheet.
- Only open and respond to legitimate e-mails. Never open an attachment from an unknown source.
- The same rules apply for classified e-mails.



Printed Materials

- Verify printer location prior to printing a document containing PII.
- Ensure "FOR OFFICIAL USE ONLY (FOUO) – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties" is prominently marked on the bottom of all documents containing PII."
- As a best practice transport/hand carry PII documents in a double wrapped container/envelope and use a "Privacy Act Data Cover Sheet" (DD Form 2923).
- Safeguard all documents when not in your direct possession by prohibiting access to 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 e-mail, badge number).
- Use a "Privacy Act Data Cover Sheet" (DD Form 2923) for all faxes that contain PII.
- Verify receipt by the correct recipient.
- External customers should be encouraged to use the US Postal Service or another secure means (i.e., encrypted e-mails or Safe Access File Exchange (SAFE)).

Scanning

- Scanned documents shall be transmitted using a secure means (i.e., digitally signed and encrypted e-mails 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 e-mail" may be used only if the sender can verify that the intended recipients have an official need to know to access the scanned file and that the e-mail 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 have an official need to know to have access to the scanned file or network share location.

Official Forms

- Use only official forms (i.e., those that have a DoD, DON, or other government number).
- Forms that collect PII from an individual must have a Privacy Act Statement (PAS).
- All DON forms must be registered on Naval Forms Online.

Electronic Storage Media

Classified and unclassified electronic storage media including: CDs/DVDs, removable and external hard drives, flash based storage media and hard drives contained in laptops, printers, copiers, scanners, MFDs, and hand held devices, must be physically destroyed.

- 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 or folders containing PII, ensure that controls are in place restricting access to only those with an official need to know.
- 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.

Shredding

- Always use a cross cut shredder or contract with a GSA approved shredder service." Strip shredders do not adequately render documents "beyond reconstruction".
- Residue size: As a best practice refer to NIST Special Publication 800-88.



Disposal

- Records should be rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation).
- Do not discard documents containing PII in trash or recycle bins.
- Burn bags can be used to dispose of PII.

Definition of PII

The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. Information that is not PII can become PII whenever additional information becomes available that would make it possible to identify an individual. Context can also cause information that would not normally be considered PII to become PII.

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 or contractor 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. 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)
- SSN Reduction: DON CIO Washington DC 151450Z MAR 17; DON CIO Washington DC 081745Z NOV 12; DoDI 1000.30
- E-mail: DON CIO WASHINGTON DC 032009Z OCT 08 and SECNAVINST 5211.5 (Series)
- 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: See the DON CIO web site for the most recent policy.
- DON Breach Reporting: DON Breach Response Plan