DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY
PSC 817 BOX 1
FPO AE 09622-0001

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION (PII) AND PRIVACY ACT DATA

27 DEC 2011

Safeguarding personally identifiable information is the responsibility of everyone. Make this your priority!

During the past year, the Department of the Navy experienced numerous inadvertent releases of PII. This compromised the identity of our people and their families. Careless loss or compromise of PII not only leads to identity theft and other criminal behavior, but prevents our people from focusing on daily tasks and overall mission. We rely on our people to accomplish the mission; they rely on those that have access to their PII to safeguard it. This is a leadership responsibility. Human error causes eighty percent of PII breach. Therefore, the focus on non-technical solutions is essential. To that end, all concerned must combine technical and non-technical solutions to include training and process improvement. This issue degrades individual and unit readiness. Communication, awareness and training are fundamental in resolving inadvertent compromise of PII.

PII should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in civil and criminal penalties. If you are not the intended recipient or believe you have received information in error, do not copy, disseminate or otherwise use the information. The Official policy is as follows:

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, medical information, and civilian National Security Personnel System (NSPS) data.

COLLECTING PII. If you collect, maintain or use Personally Identifiable Information, it must be needed 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, 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 kept secure and protected.

-Minimize the use, display or storage of SSNs and other PII whenever possible.

-Keep the information timely, accurate and relevant to the purpose for which it was collected.

-Allow only those personnel with "a need to know" to access PII.

-Immediately notify your supervisor if you suspect or discover that PII has been lost or compromised.

NAVSUPPACT NAPLES POLICY ON PERSONALLY IDENTIFIABLE INFORMATION (PII) AND PRIVACY ACT DATA

PROTECTIVE MEASURES

IT Equipment

-Never leave your laptop unattended.

-Keep your laptop in a secure government space or secured under lock and key when not in use.

-Laptops and mobile electronic equipment must have full disk encryption.

-Mark all external drives or mobile media with "FOUO, Privacy Sensitive."

-As a best practice, do not create, store or transmit PII on IT equipment when the information is not encrypted.

-Ensure PII resides only on government furnished IT equipment.

-Never store PII on personal 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 using DoD-approved certificates.

-As a best practice, ensure the e-mail subject line contains "FOUO Privacy Sensitive" if the document contains PII.

-Ensure the body of the e-mail contains the following warning, "For Official Use Only. Privacy Sensitive Information. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

-Double check that you have the correct e-mail addresses before sending.

-Double check your attachment to make sure you have selected the right document.

-Phishing is a growing concern, ensure you open and respond to legitimate sources only.

Printed Materials and Fax Machines

-Verify printer location prior to sending a document containing PII to the printer.

-Promptly pick up all copies of the documents as soon as they are printed.

-Double check the fax number prior to faxing documents with PII.

-Ensure someone is standing by on the receiving end of the fax.

-Ensure all printed documents with PII are properly marked with "FOUO, Privacy Sensitive."

-As a best practice, transport/hand carry PII documents in a double wrapped container/envelope. Use a DD Form 2923 "Privacy Act Data Cover Sheet" as a cover.

Disposal

-Dispose of documents containing PII by making them unrecognizable by shredding or burning.

-As a best practice, prior to turn in, ensure all hard drives are properly marked, physically destroyed, and actions documented.

-Do not discard documents containing PII in trash or recycle bins.
-Copiers and printers use hard drives and must be properly sanitized.

Network Shared Drives

-Make sure that controls are in place to limit access to files/folders that contain PII to those with a "need to know."
-Limit storage of PII on shared drives and folders whenever possible.
-Delete files containing PII in accordance with the SECNAV Records Management Manual.
-Verify that access controls are restored after maintenance.

COMPLIANCE All DON personnel who handle PII must complete annual PII training, and the command must maintain auditable certificates of completion. All offices that handle PII must complete a Compliance Spot Check twice yearly, and the command must maintain auditable records.

REPORTING INCIDENTS

-Contact your Privacy Act Coordinator (staff judge advocate), the NSA Admin Office or your immediate supervisor as soon as you suspect or have an actual loss or compromise of PII.
-If your PII is compromised, monitor financial accounts for suspicious activity.
-If your identity is stolen, immediately contact the Federal Trade Commission (FTC) for more information.

PRIVACY ACT. Due to the outstanding number of identity thefts that have affected the Department of Defense, The Secretary of the Navy mandated in reference that the use of Social Security Numbers of military members and civilian employees in routine correspondence was to be strictly limited. The only time that an exception is authorized is if the use of the number is essential for identification and authorized for use by authority of Executive Order 9397. An additional method is only to use the last four numbers e.g. XXX-XX-1234.

The storage of documents that may contain full Social Security Numbers should be in a secure, controlled location such as a safe or, at the very minimum, a locked drawer. Work spaces should be sanitized at the end of a work day to ensure that no Privacy Act information is left out unattended.

It is essential that this regulation be strictly adhered to in order to protect the identities of our service members and civilian employees.

C. S. GRAY