13 Jul 2012
District Five Northern Region (dpa-n)

SAFEGUARDING
PERSONALLY IDENTIFIABLE INFORMATION (PII)
BEST PRACTICES

- The Privacy Act of 1974 was created in response to concerns about collection, use, and accuracy of sensitive/personal data pertaining to individuals, such as PII. PII is data that can be used to distinguish or trace a person's identity, or any other personal information that can be linked to a specific individual. Examples of PII include: name, home mailing address, telephone number, social security number, home e-mail address, biometric identifiers (e.g., fingerprints), any unique identifying number or characteristic, and other information where it is reasonably foreseeable that the information will be linked with other personal identifiers of the individual.

- In accordance with the AUXMAN, improper treatment and handling of Auxiliary correspondence and PII include but are not limited to posting of incorrect addresses, use of incorrect mailing labels, forwarding such to individuals who do not have a need to know the information, and inappropriately posting such to the internet (e.g., Fred's Place, Military.com, blogs). Auxiliarists should expect to be held accountable for deviation from these provisions within the allowances of Chapter 3 of this Manual.

- Some PII is not **"sensitive"**, such as the PII on a business card. Other PII is Sensitive Personally Identifiable Information (Sensitive PII), such as a Social Security number or alien number, and requires stricter handling guidelines because of the increased risk to an individual if compromised.

- DHS defines "**Sensitive"** PII as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. An example of Sensitive PII is a new member enrollment package.

- As Flotilla Commanders or other Auxiliary Leaders or Staff Officers, you may manage PII of other Auxiliarists. Also, as Program Staff Officers such as a Vessel Examiner, you may be handling PII of the boating public.

- In every case, Auxiliary members must ensure all personal information is not shared with anyone unless absolutely necessary in the performance of your duties. Do not discuss another individual's **PII** unless they have a need to know.

- Do not create unnecessary or duplicate Sensitive PII. If you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy it when no longer

needed. Return incomplete forms containing PII to the individual for their retention or disposal at their discretion. There are only a few occasions when files must be kept. When this is the case, store it in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.

- The Information and Life Cycle Management Manual, COMDTINST M5212.12 (series) provides policies and procedures for administering Auxiliary records, forms, and reports program as they relate to the life cycle management of both paper and electronic documents/data.

- Do not dispose of **PII** in recycling bins or regular trash unless it has first been shredded.

- When PII information must be mailed, ensure information is properly packaged and sent in accordance with the AUXMAN chap 5 e.2.a. Mail Sensitive PII materials using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (e.g., DHL). If an Auxiliarist or Auxiliary unit desires additional protection and accountability that may be afforded by using other than the United States Postal Service (e.g., commercial express carriers like FedEx, UPS), registered/certified mail), then the time and cost associated with the use of those systems shall be the responsibility of the Auxiliarist or the Auxiliary unit.

- Do not **email** PII unless absolutely necessary. When you are emailing Sensitive PII, encrypt the e-mail using "message options" in outlook, or use an encrypted attachment with the password provided separately (e.g., by phone or in person). As a last resort, the password can be sent in a separate email, but never in the same email containing the attachment. See reference A, appendix A for additional info.

- Contact DIRAUX staff **prior** to faxing PII information to DIRAUX to ensure someone is there and ready to receive it**.**

- Loss of control, breach, compromise, unauthorized disclosure/ acquisition/access is considered a Privacy Incident where unauthorized users have access or potential access to PII. Report any unauthorized disclosures of personal information to your leadership immediately who should then contact DIRAUX.

REFERENCES:

(a) AUXILIARY MANUAL, COMDTINST M16790.1 (series) chap 5, section E.
(b) http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf
(c) http://cgweb.comdt.uscg.mil/CGDirectives/CI/CI_5260_5.pdf