What is the purpose of the Privacy Act?

The Privacy Act of 1974 provides protection for individuals against an invasion of personal privacy by Federal Agencies and establishes certain rights when Federal Agencies collect their information.

What information is covered by the Privacy Act?

Personally identifiable information (PII) under the control of a DoD Component and maintained in a system of records is protected by the Privacy Act.

PII is information that can be used to distinguish or trace an individual's identity such as their name, SSN, biometric records and other personal information which is linked to a specific individual.

What is a system of records?

Any group of records from which information is retrieved by the name of the individual or other personal identifier is referred to as a system of records.

What is a system of records notice (SORN)?

A SORN is a notice published in the Federal Register informing the public how the Department will collect, use, maintain, and disseminate PII on individuals.

Office of the Secretary of Defense
Office of the Deputy Chief Management Officer
Attn: Chief, Defense Privacy and Civil Liberties Division
9010 Defense Pentagon
Washington, D.C. 20301-9010

(703) 571-0070

http://dpcld.defense.gov

www.facebook.com/dpcld_official

www.twitter.com/DPCLD

The Privacy Act: Why it Matters to You

THINK PRIVACY

What is a Personally Identifiable Information (PII)?

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual.

Protect Your PII

IT Equipment

- Never leave your laptop unattended.
- Keep your laptop in your possession, in a secure government space, or under lock and key when not in use.

E-mail

- Ensure the body of the e-mail containing PII includes the following warning:

  FOR OFFICIAL USE ONLY—PRIVACY ACT SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.

- Ensure you are sending the e-mail to the correct recipients and all have an official need to know.
- Ensure you know if your attachments contain PII before sending, and protect it as necessary.

Network Shared Drives

- For files/folders containing PII, ensure controls are in place restricting access to only those with an official need to know.
- Limit storage of PII on shared drives whenever possible.

Agency's Responsibilities Include

When collecting information about individuals

Collect only the minimum amount of information necessary to accomplish an authorized purpose.

Maintain only information that is:

• Complete • Accurate • Timely • Relevant

Whenever collecting PII directly from an individual, provide a Privacy Act Statement that includes the following:

- The authority for the collection of personal information.
- The purpose for which the information is intended.
- Any routine uses of the information.
- Whether the provision of the information is voluntary or mandatory.
- The effects, if any, of not providing all or any part of the requested information.

Ensure accurate and up-to-date system of records notices (SORNs) are published in the Federal Register.

Allow individuals access and the opportunity to correct records about themselves when those records are maintained in a Privacy Act system of records.

Establish administrative, physical, and technical safeguards, i.e., administrative: policies and training; physical: locks and secure spaces; and technical: data-at-rest (DAR) encryption for laptops.

When information is breached

A privacy breach results when there is an actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII.

Examples of breaches include improper access to PII by personnel without an official need to know; computer hacking; the loss of paper records; and the theft of laptops containing PII.

Upon suspicion of or awareness of an actual breach:

Report to:	U.S. Computer Emergency Readiness Team (US-CERT)	Within 1 hour of discovering that a breach has occurred.
	Senior DoD Component Privacy Official	Within 24 hours
	Defense Privacy and Civil Liberties Division	Within 48 hours
Notify:	Affected individuals (those whose risk of harm has been determined to be high)	As soon as possible but no later than 10 working days after a breach is discovered and the identities of the individuals are known.