What is the Privacy Act of 1974?

It is intended to balance the Government's need for information against the individual's right to privacy. Intended to:

- Give individual's access to records kept on them
- Allow individuals to correct errors
- Limits information that is collected to what is relevant and necessary
- Restricts access to third parties
- To provide remedies for non-compliance

"What is considered 'personally identifiable information'"..?

Personally Identifiable Information (PII) is personal information maintained by an agency which is used to distinguish or trace an individual's identity, or linkable to a specified individual such as their **name, SSN, date and place of birth, mother's maiden name, biometric records, driver's license number and other ID numbers, age, race/ethnicity, gender, mailing/home address, marital status, personal cell phone number, medical, demographic and financial information, criminal or employment history, etc.** If above list is combined with additional information, it could be PII.

- **Know what constitutes PII**
- **Protect PII assessable to you at work**
- **Protect your own and others PII**

Protect It and Report the Loss of It

***Access Control*:** Access control is one of the measures taken to ensure Information Systems (ISs) are protected against threats and vulnerabilities. Identification and authentication techniques and procedures are used to control ISs access. The two IS access control methods used are the Common Access Card (CAC) with a Personal Identification Number (PIN) or a username with password.

SharePoint and shared drives continue to be the main source of PII breaches. PII should NOT be stored on shared drives or SharePoint unless it is locked down properly and only viewable by those with a need-to-know.

If PII doesn't need to be stored on these locations, then don't put it on there!

Protective Measures

Physical Protection:

- Use PA Cover Sheets (DD2923)
- Check copiers, printers or fax machines
- After hours or vacant office – lock it up!

Ground mail:

- No see-through envelopes
- Never use "holey joes"
- Never indicate contents contains PA protected data

Disposal Methods

- May include: tearing, burning, pulping, pulverizing, shredding (must be a GSA approved shredder)
- Use any reasonable means that prevents inadvertent compromise!
- A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.
- *DO NOT just throw in trash!!!!*

DoD ID Numbers

- The DoD's efforts to reduce the use of the SSN was to replace it with the number known as the Electronic Data Interchange-Personal Identifier (EDI-PI) because it presents a lower risk.
- As detailed in DODI 1000.30, "Reduction of the Social Security Number (SSN) Use Within DoD", exposure of the DoD ID Number shall not be considered a breach when exposed as part of a DoD business function.

Digital Signatures & Encryption of Email

Only official messages should be encrypted or digitally signed when transmitted. Digital signatures shall be used whenever it is necessary for the recipient to be assured of the sender's identity, have confidence the message has not been modified or when non-repudiation is required.

Messages with URL links included in the email require a digital signature.

Continued →

Emails containing Personally Identifiable Information must be encrypted. Examples are orders, payroll, finance records, recall rosters, etc. Do not send to commercial email addresses.

DSET Add-In in Outlook® will automatically include the classification at the beginning of the subject line, i.e. (FOUO) and the Privacy Act Statement as the first line in the body of the message.

DO NOT include the statement on every email you send. Just on email messages that contains PA/FOUO data.
Note: Encryption increases bandwidth and resource requirements, therefore use it correctly.

If you need to send PA/PII to a non .mil email, use the DOD SAFE (Safe Access File Exchange) to safely transfer files. The site can be located at: https://safe.apps.mil/

What is a "privacy breach" or "incident"?

Referencing AFI33-332, para 3.1.1, Per OMB Memorandum 17-12, "A PII breach is defined as loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."

PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCEDURES		
PII INCIDENT REPORTING AID		
OPSEC - Do not discuss/transmit critical information over unauthorized systems		
Responsible Entity	**Action Required**	**Time Frame From Discovery**
Individual discovering incident	Notifies Base Privacy Manager **immediately**	**Immediately**
Base Privacy Manager	Reports incident to US CERT at http://www.us-cert.gov	**1 hour**
Base Privacy Manager	Provides preliminary incident report to the following: 1st O-6 in chain of command where incident occurred or Base Commander (depending on level of breach) AF Installation & Mission Support Center (AFIMSC)	**Immediately after reporting to US Cert**
Base Commander or designee	Appoints individual to conduct PII investigation (MSgt or higher).	**24 hours**
Investigator (Base Privacy Manager or 3rd party)	Conducts and completes Investigation report using Incident Report Template-- route through base legal and base CC or designee	**72 hours**
Base Privacy Manager	Submits completed PII Incident report to AFIMSC.	**24 hours from investigation completion**
Base Privacy Manager (Risk assessment) Base Commander or designee (individual notification)	Completes risk assessment (table 1, OSD Memo, 25 Sep 08, appendix A) and if applicable, all affected individuals are notified within 10 business days of incident discovery (template letter in DoD 5400.11-R AP2, Appendix 2)	**10 business days**
Need help?	Contact the KMC office at DSN 784-1011 or Comm 315-784-1011	

FOUO (Not to be disclosed outside DoD without permission)

Quick Guide to Safeguarding

PERSONALLY IDENTIFIABLE INFORMATION

51 CS/SCXK
Building 949, Rm 229
Osan AB, ROK 96266
Commercial: 0505-784-1011
DSN: 315-784-1011

Knowledge Management Center
Office Hours:
M-F: 0700 - 1600

Discovered a breach?
Notify the Osan AB Knowledge Management Center **immediately**

https://osan.eis.pacaf.af.mil/51FW/51MSG/51CS/SCX/OKMC/BRM/PA/SitePages/Home.aspx

References for additional information:
Privacy Act of 1974
DoD 5400.11-R
AFI 33-332, AF Privacy and Civil Liberties Program
DoD Privacy Act Home Page
http://www.defenselink.mil//privacy