186th Air Refueling Wing

Privacy Act,
Personally Identifiable Information
and Protected Health Information

Calvin May, Maj
484-9611
Calvin.l.May.mil@mail.mil

Tony Grice, CMSgt
484-9733
Tony.w.grice.mil@mail.mil

Christopher Galyean, MSgt
484-9752
Christopher.f.Galyean.mil@mail.mil

PII/PA Awareness

- **The foundation for Privacy Act/PII is**

➢ **The collection and use of personally identifiable**

- **information (PII);**

➢ **Ensuring that private information collected is**

- **used for a mission requirement only**

➢ **“THE NEED TO KNOW”**

PII/PA Awareness

Examples of *Personally Identifiable Information (PII)*

- **Names (First and Last)**
- **Social Security Numbers**
- **Truncated SSN (Last 4)**
- **Driver's License Number**
- **Date of Birth**
- **Place of Birth** **(Any two together)**
- **Home Address**
- **Personal Email address**
- **Telephone Number (home/cell)**
- **Spouse Information**
- **Mother Maiden Name**
- **Mother Middle Name**
- **Employment Information**
- **Medical Information** ***Any Information that is LINKED or***
- **Financial Information** ***LINKABLE to an individual***

PII/PA Awareness

Is any PII releasable “without consent”?

Yes, the following is releasable without consent of the member:

- ✓ Name
- ✓ Rank
- ✓ Grade
- ✓ AFSC
- ✓ Office Address
- ✓ Office phone number
- ✓ Unit Address
- ✓ Biographies of key personnel

For more information see AFI 33-332 Para 2.12

PII/PA Awareness

Possible Locations of PII

- **Computer (data storage) and shared drives (G drive, O drive, etc)**

- **Physical Records**
- **Email**

NOTE: Ensure proper security permissions are set to protect personal data placed on Shared drives, Internet or storage.

PII/PA Awareness

PII Collections have Legal Requirements

- System of Records Notice
- Privacy Impact Assessment
- Appropriate safeguards
- Informing people at time of collection
- How the Information is used must match why it was collected
- Rules around sharing
- Requirements apply regardless of how/where PII is stored
- Personal Liability for violating some legal requirements

KEY Takeaways:

- Don’t accidentally create a System of Records
- Keep informed about the data you are responsible for
- Consult with your PA Officer to ensure all obligations are addressed

PII/PA Awareness

Email Messages that contain PII

@ Use Common Access Card procedures

@ Encrypt email when possible

See AFI 33-119, AF Messaging, Chapter 2

@ Announce in the subject line that FOUO information is being sent Add PA Notification in the first line of your email

See AFI 33-332, AF Privacy Program, Chapter 2

@ Do not indiscriminately apply the PA Statement to any/all emails!

Use it only in situations when you are actually transmitting personal information

See AFI 33-332, AF Privacy Program, Paragraph 2.5.7

PII/PA Awareness

PII Breaches

- Breaches must be reported to the US CERT within one (1) hour of discovery
  - Source Office of Management and Budget Memorandum M-06-19
- AF takes PII breaches very seriously – breaches must be reported to the
- Privacy Act Chain of Command within 72 hours of the incident
  - Source Department of Defense 5400.11-R, Department of Defense Privacy Program
- Individuals affected by a breach must be notified within 10 working days
  - Source Department of Defense Memorandum June 05, 2009, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)"
- Risk of Harm should be assessed before issuing notification
- **Is every mistake automatically a breach?—NO**
- **EXAMPLE:**
  - After hours, a letter with an individual's SSN is left out in the commander's support staff's office.
  - The First Sergeant finds the letter and see's the individuals SSN. This is NOT A BREACH … the First Sergeant already has access to individuals SSN.
  - If someone else had seen this letter (who did not have a need to know) it WOULD be a breach.

PII/PA Awareness

Tips to Avoid PII/PA Breaches

1. Take PII/PA seriously!

2. Respect the privacy of others

3. Follow need to know principle…share with those specific DoD employees who the data to perform official, assigned duties
   - If you have doubts about sharing data, consult with your supervisor, your PA Officer, the BRM office, or the AFIs

4. Don't create new PII collections without meeting proper requirements

5. Report to your chain of command anytime you see personal data left unattended

6. Know the PA requirements
   - Refer to the following AFI 33-332, PA Program which implements DoD 5400.11, DoD Privacy Act Program; and DoD 5400.11-R, DoD Privacy Program

PII/PA Awareness

For More Information

- ✓For additional guidance, Information, Inquires, and or questions contact your BRM or PA Monitor
- ✓You can also visit the BRM EIM site for further guidance and/or training
- ✓Your base Privacy Act Officer is in the Base Records Management Office, 484-9752