

**2011 PRIVACY 101: Orientation  
Training for all Military  
Members, Civilian Employees,  
and Contractor Personnel**

# Why You Are Being Asked to Take this Training

- We continue to receive reports of data breaches as a result of poor practices/protocols
- Handling breaches costs time and money
- We don't want you to be accused of carelessly handling personal data!

# What is the Privacy Act (PA)?

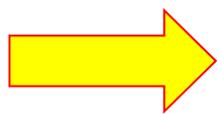
- **The Privacy Act limits an agency's ability to collect and share personal data. The Privacy Act requires that all Executive Branch Agencies follow certain procedures when:**
  - **Collecting personal information**
  - **Creating databases containing personal identifiers**
  - **Maintaining databases containing personal identifiers**
  - **Disseminating information containing personal data**

# What are some examples of Privacy Data?

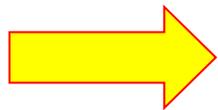
- **Personal data about individuals, such as:**
  - Financial, credit, and medical data
  - Security clearance level
  - Leave balances; types of leave used
  - Home address and telephone numbers (including home web addresses)
  - Social Security Number
  - Mother's maiden name; other names used
  - Drug test results and any information pertaining to participation in rehabilitation programs
  - Family data
  - Religion, race, national origin
  - Performance ratings
  - Names of employees who hold government-issued travel cards, including card data

# What are the limitations of the Privacy Act?

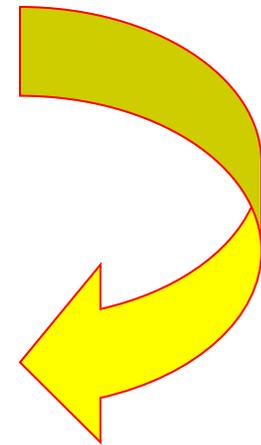
The Privacy Act applies only to:



**US citizens**  
or



**Lawfully admitted aliens**



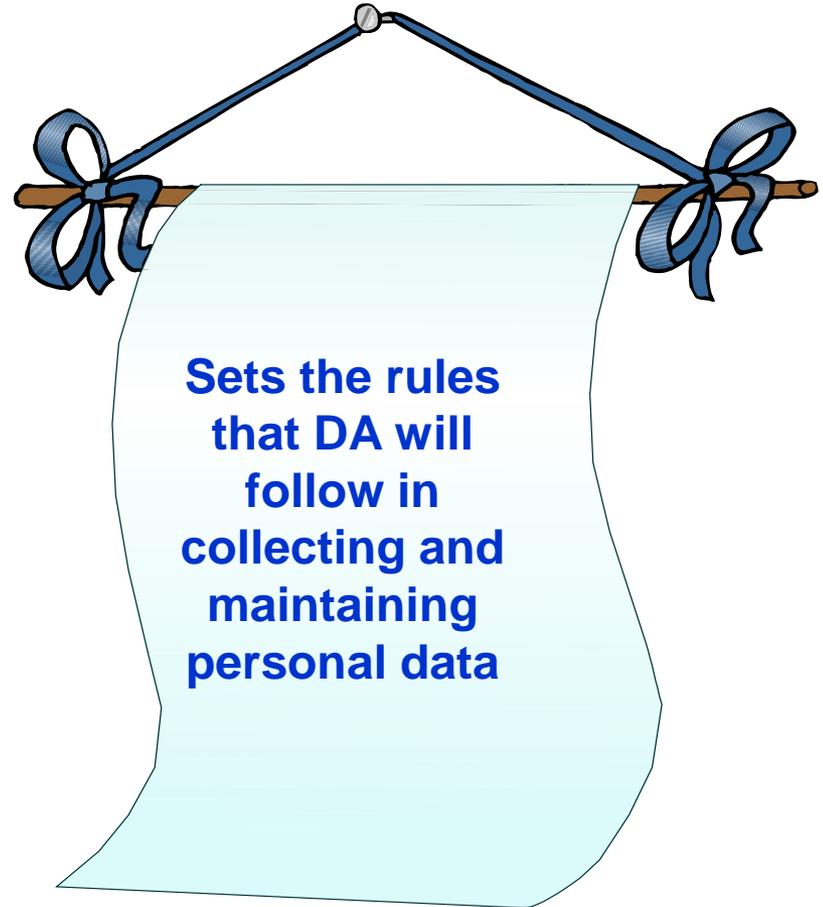
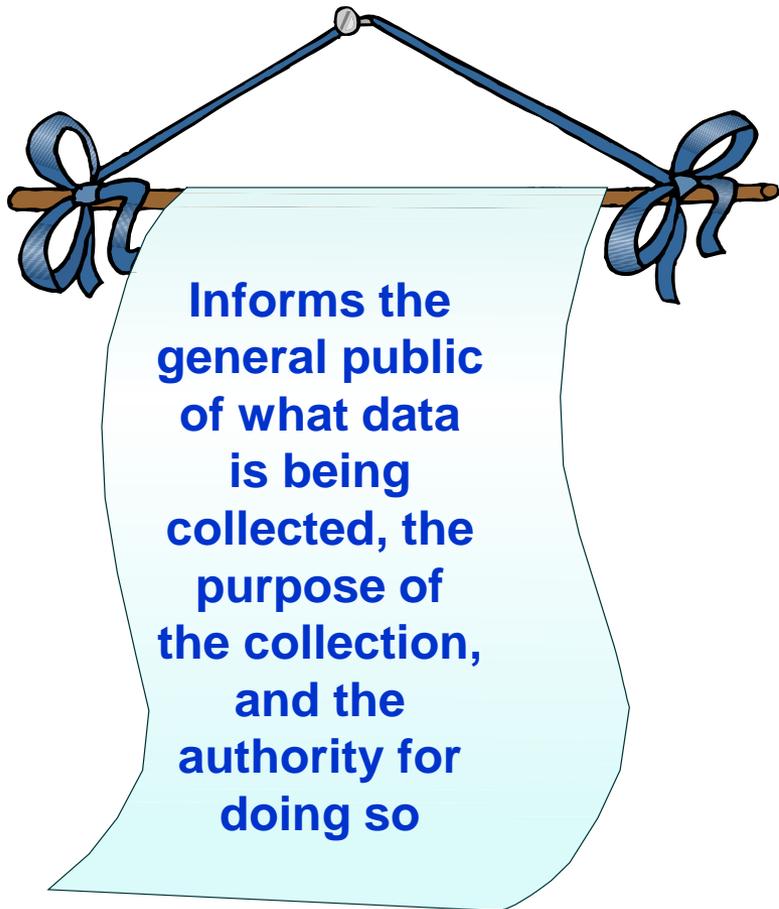
**Whose records are filed in a  
“System of Records” where those records are  
retrieved by a personal identifier.**

# What is a System of Records?

- **A System of Records is a group of records that:**
  - **Contains a personal identifier (such as a name, Social Security Number, Employee Number, etc)**
  - **Contains one other item of personal data (such as home address, performance rating, blood type, etc)**
  - **Is retrieved by a personal identifier**

# What purpose does the System Notice serve?

- **A System Notice:**



# **ARMY PA RESPONSIBILITIES**

- **Establish rules of conduct for collecting, maintaining, and distributing personal information.**
- **Publish PA system of records notice in the Federal Register.**
- **Collect only data that is authorized by law.**
- **Share data with only those individuals having an official need-to-know.**

# **ARMY PA RESPONSIBILITIES**

- **Establish and apply data safeguards.**
- **Allow individuals to review records about themselves.**
- **Allow individuals to amend their personal records regarding factual information that is in error.**
- **Keep a record of disclosures made outside of DOD to authorized routine users described in the PA system notice.**

# **ARMY PA RESPONSIBILITIES**

- **Upon written request, provide a copy of the record to the subject of the file.**
- **Maintain only accurate, timely, and complete information.**
- **When directly soliciting personal information, provide a PA statement that addresses the authority for the collection, purpose for the collection, routine uses that will be made of the information, and whether collection is voluntary or mandatory.**

# **ARMY PA RESPONSIBILITIES**

- **Follow the guidance set forth in the PA systems notice regarding release/withholding of information.**
- **With some exceptions provided for in the PA, make no disclosure of information without the record subject's written consent.**
- **When contracts are awarded that involve PA data, ensure the contract contains the appropriate Federal Acquisition Regulation (FAR) privacy clauses.**

# **WHAT ARE YOUR RESPONSIBILITIES?**

- **As an employee, you play a very important role in assuring DA complies with the provisions of the Privacy Act. Accordingly,**
  - **DO NOT collect personal data without authorization**
  - **DO NOT distribute or release personal information to other employees unless you are convinced they have an official need-to-know**

# **WHAT ARE YOUR RESPONSIBILITIES?**

- **DO NOT** be afraid to challenge “anyone” who asks to see PA information for which you are responsible.
- **DO NOT** maintain records longer than permitted.
- **DO NOT** destroy records before disposal requirements are met.
- **DO NOT** place unauthorized documents in PA systems of records.

# **WHAT ARE YOUR RESPONSIBILITIES?**

- **DO NOT commingle information about different individuals in the same file.**
- **DO NOT transmit personal data without ensuring it is properly marked. Use 'FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE.'**
- **DO NOT use interoffice envelopes to mail Privacy data.**
- **DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet.**

# **WHAT ARE YOUR RESPONSIBILITIES?**

- **DO NOT** create a new system of records without first consulting your Privacy Officer.
- **DO NOT** hesitate to offer recommendations on how to better effectively manage privacy data.

**YOUR INSIGHT COUNTS! YOUR DEDICATION TO PROTECTING PRIVACY IS PARAMOUNT TO DA SUCCESS!**

# Disposing of Privacy Data

- **Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.**
- **Don't dispose the data in regular trash.**
- **Don't dispose the data in recycle containers unless the information being recycled has been or will be shredded.**

# Disposing of Privacy Data

- **Disposal methods may include:**
  - **Tearing**
  - **Burning**
  - **Melting**
  - **Chemical decomposition**
  - **Pulping**
  - **Pulverizing**
  - **Shredding**
  - **Mutilation**

# **CONTRACTOR PERSONNEL**

- **Because the Army is a blended workforce, we must ensure that our contractors understand that they too must comply with our Privacy Program and follow the same rules as government employees.**

# PENALTIES

- **The Privacy Act contains criminal penalties for knowing and willfully:**
  - **Obtaining records under false pretenses;**
  - **Disclosing privacy data to any person not entitled to access;**
  - **Maintaining a system of records without meeting public notice requirements.**
- **Result: Misdemeanor criminal conviction and a fine of up to \$5,000.**

# **PENALTIES**

- **Courts may also award civil penalties for:**
  - **Unlawfully refusing to amend a record;**
  - **Unlawfully refusing to grant access to a record;**
  - **Failure to maintain accurate, relevant, timely, and complete information;**
  - **Failure to comply with any PA provision or agency rule that results in an adverse effect on the subject of the record.**

**Penalties for these violations include:**

**Actual damages;**

**Payment of reasonable attorney's fees;**

**Removal from employment.**

# **HOW WILL I KNOW IF THE DATA THAT I HANDLE IS PRIVACY ACT PROTECTED DATA?**

- **Privacy data should be marked: “For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties.”**
- **Be aware that privacy data may not always be marked as such. If you have any questions about whether data is protected under the Privacy Act, ask your supervisor.**

# **THINK PRIVACY**

- **YOUR ATTENTION TO PRIVACY SERVES EVERYONE!**
- **FACTOR PRIVACY IN YOUR WORKPLACE.**
- **DEVELOP BEST PRACTICES.**
- **PLEASE DIRECT ANY QUESTIONS TO YOUR PRIVACY OFFICER, PATRICIA KELLY-JOHNSON, 751-5335, PATRICIA.KELLYJOHNSON@CONUS.ARMY.MIL**

# TEST

- Circle the correct answer.
  
- 1. What are examples of Privacy Data?
  - (a) Home address and telephone number
  - (b) Work week
  - (c) Work phone number
  
- 2. The Privacy Act applies only to:
  - (a) All foreigners
  - (b) All Fort Jackson employees
  - (c) US Citizens and lawfully admitted aliens
  
- 3. How should you dispose of Privacy Data?
  - (a) Place it in regular trash
  - (b) Take it home
  - (c) Shred, burn or tear

# CERTIFICATE OF INITIAL/ANNUAL REFRESHER TRAINING FOR PRIVACY ACT

This is to certify that I have received/completed initial/annual refresher training on my privacy and security responsibilities as addressed in Privacy 101. I understand that I am responsible for safeguarding Personally Identifiable Information (PII) that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard PII, for improperly using or disclosing PII, and for failure to report any known or suspected loss of PII or the unauthorized disclosure of such information.

---

(Signature)

---

(Print Name)

---

(Date)

---

(Office)