



Privacy Act  
&  
Safeguarding Personally  
Identifiable Information  
Training

# Course Introduction

Welcome to the Privacy Act (PA) and Safeguarding Personally Identifiable Information (PII) Refresher Training Course.



# Training Requirements

- This training is required under DoD 5400.11-R, DoD Privacy Program; OMB Circular A-130, Managing Information as a Strategic Resource; and OSD Administrative Instruction 81, DoDEA Privacy Program.
- All DoDEA employees are required to complete this training. Contractor employees having computer access must also complete this training.
- This course contains several multiple-choice knowledge check questions. When responding to these questions, please choose the BEST response.
- In order to receive credit for completion of this training, employees must complete the certificate that is provided at the end of the course and submit it through their appropriate supervisor.

# Overview of the Privacy Act of 1974

The main points that will be covered in this course are:

- Statutory/Regulatory Authority
- Purpose of the Privacy Act
- Policy Objectives
- Definitions
- System of Records Notice (SORN) and Privacy Act Statement (PAS)
- Social Security Number (SSN) Reduction Program
- Disclosure
- Accessing and Amending Records
- Safeguarding Personally Identifiable Information (PII)
- Phishing
- Teleworking with PII
- Criminal and Civil Penalties
- Tips
- Your Roles and Responsibilities
- Contact information

# Statutory/Regulatory Authority of the Privacy Act

- Statutory and Regulatory Authority for the Privacy Act is established through the following:
  - The Privacy Act of 1974, as amended (5 U.S.C. 552a);
  - OMB Circular A-130;
  - OMB Circular A-108;
  - DoD Directive 5400.11;
  - DoD Regulation 5400.11-R; and
  - OSD Administrative Instruction No. 81.



# Purpose of the Privacy Act

- Established a Code of Fair Information Practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
- Restrict disclosure of personally identifiable records maintained by agencies.
- Grant individuals increased rights of access to agency records maintained on themselves.
- Allows individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

# Four Basic Policy Objectives

- Restrict disclosure of personally identifiable records maintained by agencies.
- Grant individuals increased rights of access to agency records maintained on themselves (first party access rights).
- Allows individuals the right to seek amendment of records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
- Establish a Code of Fair Information Practices which requires agencies to comply with statutory norms for collection, maintenance, use, and dissemination of records.

# Definitions

- **Individual** -- A citizen of the United States or an alien lawfully admitted for permanent residence:
  - Deceased individuals do not have any Privacy Act rights, nor do executors or next of kin.
  - Privacy Act rights are personal to the individual who is the subject of the record and cannot be asserted derivatively by others.
  - However, an individual may authorize access to their attorney, friend, family member, etc.
- **Maintain** -- maintain, collect, use, or disseminate records contained in a system of records.
- **Personally Identifiable Information (PII)** – Information about an individual that identifies, relates, or is unique to, or describes him or her; e.g., SSN, medical information, tattoo, biometrics, date of birth, home address, telephone number.



# Definitions

- **Record** -- Any item, collection, or grouping of information about an individual maintained by a DoD Component.
- **Routine Use** – Release of information outside a Federal agency for a purpose compatible with the purpose for which the information was collected. Releases of information between DoD Agencies (i.e., Army to Navy or another DoD Component) are not considered routine uses. However, a release from the Defense Manpower Data Center to the Department of Veterans Affairs would require a routine use.
- **System of Records** – A group of records under the control of a DoD Component from which PII is retrieved by the individual's name or some other unique personal identifier.



# Types of PII

- Name/Other Names
- DoD ID Number
- SSN/Truncated SSN
- Citizenship/Legal Status
- DOB/POB
- Gender/Race/Ethnicity
- Mother's Maiden/ Middle Name
- Security Clearance
- Biometrics
- Vehicle Identifiers
- Medical Information
- Disability Information
- Financial Information
- Employment Information
- Personal Phone Numbers (Home/Cell)
- Personal email address
- Home/ mailing address
- Religious Preference
- Emergency Contact
- Marital Status
- Spouse Information
- Child Information
- Military Records
- Law Enforcement Information
- Drivers License
- Other ID Number
- Education Information
- Photo
- Tattoo

\*From DD Form 2930, Privacy Impact Assessment (PIA)

# Knowledge Check (Introduction)

## Knowledge Check Instructions

- On the next few pages, you will be provided the opportunity to check your understanding of the information presented about the Privacy Act and its primary features and definitions.
- For all Knowledge Checks, please **click** the BEST answer to the question.
- If you have **clicked** the **correct** answer, you will automatically proceed to the next question or slide.
- If you have **clicked** the **incorrect answer**, you will be redirected back to the Knowledge Check question in order to try again.

# Knowledge Check #1

Which of the following states the four objectives of the Privacy Act?

- A. Restrict first party access, right of disclosure, right of amendment, establish fair information practices.
- B. Restrict right of amendment, right of first party access, restrict disclosure of PII, establish fair information practices.
- C. Restrict disclosure of PII, increase right of first party access, increase right of amendment, and establish fair information practices.
- D. Restrict right of amendment, restrict disclosure of PII, right of first party access, establish fair information practices.

# Knowledge Check #1

**INCORRECT ANSWER**

Restrict first party access, right of disclosure, right of amendment, establish of fair information practices.

# Knowledge Check #1

**INCORRECT ANSWER**

Restrict right of amendment, right of first party access, restrict disclosure of PII, establish fair information practices.

# Knowledge Check #1

CORRECT ANSWER

Restrict disclosure of PII, increase right of first party access, increase right of amendment, and establish fair information practices.

# Knowledge Check #1

**INCORRECT ANSWER**

Restrict right of amendment, restrict disclosure of PII, right of first party access, establish fair information practices.

# Knowledge Check #2

Which of the following is **NOT** PII?

- A. DoD ID Number
- B. Medical Records
- C. Personal Cell Phone Number
- D. First Grade Teacher

# Knowledge Check #2

INCORRECT ANSWER

DoD ID Number

DoD ID Number is a form of PII.

# Knowledge Check #2

INCORRECT ANSWER

Medical Records

Medical Records contain much PII; e.g. SSN, medical history, date of birth, home address, financial information and telephone number.

# Knowledge Check #2

INCORRECT ANSWER

Personal Cell Phone Number

A personal cell phone number is a unique identifier for an individual.

# Knowledge Check #2

CORRECT ANSWER

First Grade Teacher

# System of Records (SOR)

- A Privacy Act “System of Records” is a group of records that:
  - Contains information that is retrieved by an individual’s unique identifier(s);
  - e.g. the name of the individual, date of birth, SSN, DoD ID Number, biometrics, or by some other identifying number or symbol that is unique to the individual.

# System of Records Notice (SORN)

It's the foundation of Privacy programs:

- Transparency – enables people to know what data is being collected and on whom.
- Federal rulemaking – published in Federal Register.
- A tool to answer Privacy questions.
- The authority for sharing information with others.
- A blueprint that describes the business practice.
- Reviewed on a continual basis to reflect changes in business practices.

# The SORN is a Blueprint

It provides the following information about a system:

- System Name and Number
- Security Classification
- System Location
- System Manager(s)
- Authority
- Purpose
- Categories of Individuals
- Categories of Records
- Record Source(s)
- Routine Uses
- Storage of Records
- Retrieval of Records
- Retention and Disposal
- Administrative, Technical, and Physical Safeguards
- Record Access Procedures
- Contesting Record Procedures
- Notification Procedures
- Exemptions
- History

# Collecting PII

- The goal of the Privacy Act is to directly solicit information from the individual.... Why?... Accuracy!
- When directly soliciting PII from an individual, and the record is maintained in a Privacy Act system of records, they must be provided a Privacy Act Statement (PAS), regardless of the medium used to collect the information (paper or electronic forms, personal or telephonic interviews, or other methods).
- The PAS statement enables the individual to make an informed decision whether to provide the information requested.

# Privacy Act Statements (PAS)

- The PAS should appear conspicuously on forms collecting PII and address the following five areas:
  - ✓ Authority
  - ✓ Purpose
  - ✓ Routine Uses
  - ✓ Disclosure
  - ✓ System number and name, and link to the relevant system of records notice.
- Must be made available upon request.

# Social Security Number (SSN) Reduction Program

- DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD” establishes DoD policy on the reduction and/or elimination of the use of SSNs:
  - Provides for 12 acceptable uses and requires documentation.
- If SSN collection is authorized:
  - P.L. 93-579, Section 7, provides that it shall be unlawful to deny any benefit, right, or privilege provided by law because the individual refuses to disclose his or her SSN.
  - Any time an SSN is requested, a Privacy Act Statement must be provided.

# Disclosure

- No agency shall disclose any record which is contained in a system of records to any person or another agency without a written request or prior written consent of the individual to whom the record pertains.
- Except:
  - The disclosure of the record would be to those officers and employees of the agency who have a need for the record in the performance of their duties.
  - For an established routine use to another federal agency.
- Disclosure includes any means of communication – oral, written, or electronic.
- Disclosure does not occur if the communication is to those who already know.

# Disclosing PII

- Follow the “need to know” principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.
- If the Privacy Act System Manager has granted you authority to make disclosures outside DoD:
  - Share only with those individuals and entities outside DoD that are listed in the “Routine Use” section of the applicable SORN.
- If you have doubts about sharing data, consult your supervisor, the Privacy Act System Manager, or your Component Privacy Officer.

# Knowledge Check #3

Select the answer that is **false**.

A SORN is:

- A. Required to be published in the Federal Register.
- B. Required when collected data is not retrieved by a unique personal identifier.
- C. A tool to answer Privacy questions.
- D. A blueprint that describes a business practice.

# Knowledge Check #3

**INCORRECT ANSWER**

Required to be published in the Federal Register.

# Knowledge Check #3

CORRECT ANSWER

Required when collected data is not retrieved by a unique personal identifier.

# Knowledge Check #3

**INCORRECT ANSWER**

A tool to answer Privacy questions.

# Knowledge Check #3

**INCORRECT ANSWER**

A blueprint that describes a business practice.

# Knowledge Check #4

Disclosure of information always requires written consent or a request from the individual.

[True](#)

[False](#)

# Knowledge Check #4

**INCORRECT ANSWER**

You selected **True.**

This answer is **incorrect.** Records may be disclosed to those officers and employees of the agency who have a need for the record in the performance of their duties or for an established routine use to another federal agency.

# Knowledge Check #4

CORRECT ANSWER

You selected **False.**

This answer is **correct.** Records may be disclosed to those officers and employees of the agency who have a need for the record in the performance of their duties or for an established routine use to another federal agency.

# Accessing Records

The Privacy Act allows individuals to:

- Seek access to records retrieved by their name and/or personal identifier that are contained in a Privacy Act system of records.
- Provide written authorization for their representative to act on their behalf.
- Seek records on behalf of a minor child, if they are the legal guardian or parent, acting in the best interest of the minor child.

# Amending Records

- The Privacy Act allows individuals to seek amendment of erroneous information – based on fact – not opinion.
- Procedures (established in 32 CFR Part 311):
  - Submit request in writing – except for routine administrative matters, such as change of address/phone number.
  - Include a description of the information to be amended; reason for amendment; type of amendment action sought – including all available evidence that supports the request (Burden of proof on the requester).
- Systems manager makes the call and must acknowledge receipt within 10 working days – make a ruling within 30 working days.
- If the request is denied, the requestor is notified of their right to appeal.

# Safeguarding PII

- The Privacy Act of 1974 requires agencies to:
  - Establish safeguards
  - Maintain accurate, relevant, timely, and complete information
- Types of Safeguards:
  - **Physical**
  - **Technical**
  - **Administrative**
- Program managers and IT system designers are responsible for identifying and establishing safeguards.
- PII must always be treated as “FOR OFFICIAL USE ONLY” and must be marked accordingly. This applies not only to physical records, but also to electronic (including email) transmissions and faxes, which must contain the cautionary marking “FOR OFFICIAL USE ONLY” and/or “FOUO”, whichever is appropriate for the recipient, before the beginning of the text containing the PII.

# Safeguarding PII – Physical Safeguards

- Physical:
  - Paper records should be stored in cabinets.
  - Records being faxed or mailed should have a coversheet (DD Form 2923).
  - Facilities handling PII should be access controlled and hardware should be locked up.
  - Never leave files, storage media, or computers unattended or in vehicles.
  - Use filtering devices on computer screens.
  - Records Disposal – Retirement or deletion of a record does not preclude the need for safeguards:
    - Must render discarded info unrecognizable and beyond reconstruction.
    - Destruction should be tailored to the type of media involved (e.g., paper – burn, shred; electronic – overwrite, degauss, incinerate).

# Safeguarding PII – Technical Safeguards

- Technical:
  - Encryption: Ensure all emails with PII are encrypted.
  - Remote secure access to DoD Servers.
  - Ensure records are access controlled:
    - PII on shared drives should be restricted and accessible to only those with a need to know.
  - Time-out function.
  - Log and verify.
  - Ensure SSNs (including the last 4) are not posted on public facing websites.
  - Data Loss Protection tools and PII blocking.

# Safeguarding PII – Administrative Safeguards

- Administrative:
  - Have policies in place for PII handling, specifically defining:
    - affected individuals
    - affected actions
    - consequences
  - Ensure staff handling PII are adequately trained:
    - need to know
    - commensurate with responsibilities
    - prerequisite before permitted access to DoD systems
    - mandatory for affected DoD personnel and contractors
    - ensure understanding of responsibilities
  - It is DoD policy that:
    - IT systems with PII are reviewed every three years and must be synchronized with the information system's assessment and authorization cycle (DoDI 5400.16)
    - SORNs are reviewed on a continual basis (OMB Circular A-108)
    - results reported in annual FISMA reports (OMB Annual FISMA Guidance)

# Phishing

- Phishing is an attempt to falsely obtain sensitive information, such as passwords, personal information, military operations, and credit card/financial details, by masquerading as a trustworthy person/business.
- Phishing emails not only trick you into giving out sensitive information, but can include malicious software.
- Most phishing attempts are for identity theft, but there is a rise in attempts at gaining access to online banking, federal, and defense information.
- These hidden/unknown threats can capture your passwords/login credentials and also compromise unclassified, but sensitive, information that can put the DoD at risk.

# Phishing Prevention Tips

- In order to protect your privacy, identity and interests:
  - Guard against spam.
  - Only communicate personal information via self-initiated phone calls.
  - Conduct online transactions on secure sites.
  - Beware of links in emails that ask for personal information.
  - Never enter personal information in a pop-up.
  - Regularly check online accounts and bank statements.

# Knowledge Check #5

The three types of safeguards are which of the following:

- A. Legal, physical, and technical.
- B. Physical, technical, and administrative.
- C. Administrative, technical, and security.
- D. Legal, physical, and security.

# Knowledge Check #5

**INCORRECT ANSWER**

Legal, physical, and technical.

# Knowledge Check #5

CORRECT ANSWER

Physical, technical, and administrative.

# Knowledge Check #5

**INCORRECT ANSWER**

Administrative, technical, and security.

# Knowledge Check #5

**INCORRECT ANSWER**

Legal, physical, and security.

# Teleworking with PII

- Paper records:
  - Place PII in locked drawers, locked briefcases, or other secure areas where family or household members, or other unauthorized personnel cannot access it.
- Electronic records:
  - Use CAC access and password protection protocols.
  - Do not share your CAC and password with anyone.
  - Save, store and use PII only on DoD-issued equipment (i.e., Mobi-key, DoD issued laptop).
  - Do not email work-related PII to your personal email account.
- DoD Instruction 1035.01, Telework Policy and DD Form 2946, Department of Defense Telework Agreement provide additional information for teleworkers working with PII.

# Transporting PII

- Follow the guidelines found in DoD Information Security Program: Controlled Unclassified Information (CUI) (DoD 5200.01, Vol. 4).
- Hand carrying:
  - Use DD Form 2923, Privacy Act Data cover sheet, to shield contents.
- Using Ground Mail:
  - Use Kraft or white envelopes
  - Double wrapped if appropriate.
  - Mark the envelope to the attention of the authorized recipient.
  - Never indicate on the outer envelope that the contents contain PII.

# Disposing of PII

- Federal records must be disposed of in accordance with the approved National Archives and Records Administration (NARA) retention and disposal schedule.
- Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.
- Disposal methods may include:
  - Burning
  - Melting
  - Chemical decomposition
  - Pulping
  - Pulverizing
  - Shredding
  - Mutilation
  - Degaussing



# Knowledge Check #6

When teleworking, you should:

- A. Save, store, and use PII only on DoD equipment.
- B. Leave PII accessible to family members.
- C. Email PII to your personal email account.
- D. Share your password.

# Knowledge Check #6

CORRECT ANSWER

Save, store, and use PII only on DoD equipment.

# Knowledge Check #6

- Leave PII accessible to family members. [INCORRECT ANSWER]

# Knowledge Check #6

**INCORRECT ANSWER**

Email PII to your personal email account.

# Knowledge Check #6

**INCORRECT ANSWER**

[Share your password.](#)

# Knowledge Check #7

Proper disposal methods include all of the following except:

- A. Burn bag/shredding where available
- B. Chemical decomposition
- C. Recycling
- D. Pulverizing

# Knowledge Check #7

**INCORRECT ANSWER**

Burn bag/shredding when available

# Knowledge Check #7

**INCORRECT ANSWER**

Chemical decomposition

# Knowledge Check #7

CORRECT ANSWER

Recycling

# Knowledge Check #7

INCORRECT ANSWER

Pulverizing

# Criminal and Civil Penalties

## Criminal Penalties

- Any agency official or employee who willfully makes a disclosure of a record knowing it to be in violation of the Privacy Act or maintaining a system of records without having published the required system notice may be convicted of a misdemeanor and fined up to \$5,000.
- Any person who knowingly and willfully requests or obtains a record of another individual from an agency under false pretenses may be convicted of a misdemeanor and fined up to \$5,000.

## Civil Penalties

- The Privacy Act also imposes civil penalties on violators who:
  - Unlawfully refuse to amend a record
  - Unlawfully refuse to grant access to records
  - Fail to maintain accurate, relevant, timely, and complete data
  - Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect
- Penalties may include:
  - Payment of actual damages
  - Payment of reasonable attorney's fees
  - Removal from employment



# Tips for Avoiding PII Breaches

- Take protection of PII seriously.
- Respect the privacy of others.
- Alert your supervisor or other management official when you see PII left unattended.
- Know Privacy Act requirements.
- Ensure that all message traffic, faxes, and email containing PII are properly marked and email is encrypted.
- Do not email the PII of others to a personal email account.
- Do not leave laptops or other storage media unattended.
- **Think smart!**

**HELPFUL  
TIPS**

# If You Have Access to PII

- Protect it at all times.
- Do not share with anyone unless:
  - The recipient is authorized access in the SORN.
  - The subject of the record has provided written permission to disclose it to the recipient.
- Password protect PII placed on shared drives or Component Intranet.
- Monitor your actions—if I do this, will I increase the risk of unauthorized access?

## **Remember:**

**You may be subject to criminal or civil penalties for violating the Privacy Act!**

# Your Role and Responsibility

- Do not collect PII without proper legal and regulatory authority.
- Do not maintain unscheduled files; do not maintain or release inaccurate information.
- Do not distribute or release PII to individuals who do not have an authorized need for access.
- Do not maintain records longer than authorized in your Component Records Disposition Schedule.
- Do not destroy records before authorized by the Component Records Disposition Schedule.
- Ensure unauthorized documents are not placed in a system of records.
- Ensure all documents that contain PII are marked “For Official Use Only – Privacy Act of 1974” or “FOUO – Privacy Act Data.”
- **Think “Privacy” before establishing new data collections.**

# Contact Information

**DoDEA Privacy Website:**

[www.dodea.edu/privacy.cfm](http://www.dodea.edu/privacy.cfm)

**General Inquiries:**

[Privacy\\_Forms@dodea.edu](mailto:Privacy_Forms@dodea.edu)

# Instructions for Course Credit

Congratulations!  
You have completed the training.

Please read the “Notice of Completion” on the next page, sign, and return to your Supervisor and send a copy to:

[Privacy\\_Forms@DoDEA.EDU](mailto:Privacy_Forms@DoDEA.EDU)

# Notice of Completion

This is to certify that I have received refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to in performing my official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information.

---

Signature