



PERSONALLY

IDENTIFIABLE

INFORMATON

(PII)



# PII - REFERENCES



- DOD 5400.11-R, DoD Privacy Act Program, May 07
- OSD Memo, Subj: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Sep 07
- Fort Benning Policy Memo 25-54-3, dated 29 Sep 10, Subj: Fort Benning Policy for Safeguarding and Reporting Personally Identifiable Information (PII)
- IMCOM PA Website:  
[https://www.us.army.mil/suite/portal/index.jsp;jsessionid=7454C4C5361E5044B0F81AA68743AA37.appd06\\_3](https://www.us.army.mil/suite/portal/index.jsp;jsessionid=7454C4C5361E5044B0F81AA68743AA37.appd06_3)
- DA PA Website:  
<http://www.rmda.belvoir.army.mil/rmdaxml/rmda/PrivacyActProg-Guidance.asp>



# COURSE OBJECTIVE - PII



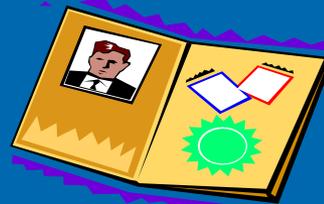
- DEFINE PII
- DEFINE PII BREACHES
- KNOW REPORTING PROCEDURES IN CASE OF LOSS OF PII
- KNOW PROPER DISPOSAL OF PII



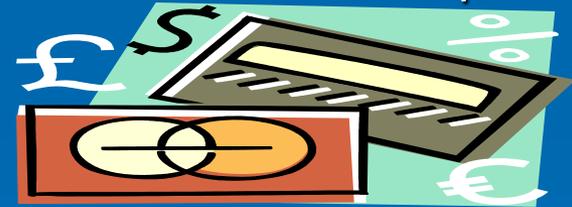


## WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)

- PII Is Any Information Which Can Be Used To Distinguish Or Trace An Individual's Identity.



- PII Is Any Personal Information Which Is Linked Or Linkable To A Specified Individual



- PII Can Be Hard Copy Or Electronic Records Stored Within Data Bases Or Other Applications On Computers, Laptops, And Personal Electronic Devices Such As Blackberries.





# WHAT ARE SOME EXAMPLES OF PII BREACHES?



➤ Lost or Stolen Mobile Computing Devices (Laptop, Blackberry, Etc.) that Contained PII

➤ Posting PII On Public-facing Websites

➤ Successful Network Intrusions

➤ Anytime Persons Gain Access To PII Without An Official Need To Know:

- On Intra-agency Websites

- Through Bulletin Boards In Common Areas

- By Distributing PII In Hardcopy Or Electronic Form

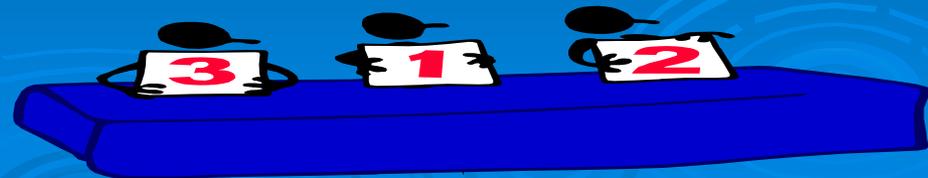
- Improper Disposal Of PII





## OTHER EXAMPLES OF PII WHEN LINKED TO AN INDIVIDUAL

- Security Clearance Level
- Leave Balances; Types Of Leave Used
- Addresses And Telephone Numbers
- Social Security Number
- Drug Test Results
- Family Data
- Performance Ratings
- Medical Condition And Treatment Information





# WHY DOES THE DEPARTMENT OF THE ARMY (DA) COLLECT PII INFORMATION?



## DA Collects PII For Several Reasons:

1. To hire You



2. To pay You



3. To locate You



4. To educate You

5. To provide services to You





# WHEN TO PROVIDE A PRIVACY ACT STATEMENT (PA)



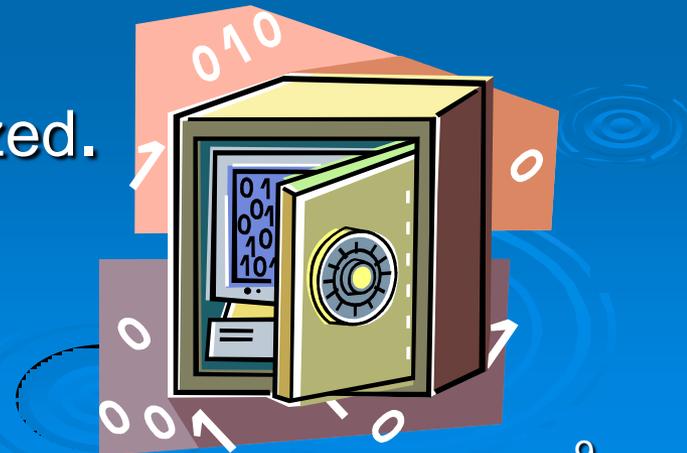
- Provide a PA statement either in writing or orally to the subject of the record when collecting Personally Identifiable Information (PII) from the individual if the collected information will go in a system of records notice (SORN). A list of SORNS is located at <http://privacy.defense.gov/notices/index.shtml>
- The PA statement is to be given regardless of how you collect or record the answers.
- A sign may be displayed in areas where people routinely furnish PA/PII information.
- A copy of the PA statement only has to be provided to the person from whom the information is collected if requested.
- Do NOT ask the person to sign the PA statement.



## WHAT ARE SOME OF YOUR RESPONSIBILITIES WITH RESPECT TO PII?



- Be able to recognize PII and safeguard it.
  - PII does not have to be from a Privacy Act System of Records –
- Only share PII with authorized personnel.
- Be aware of local physical and technical procedures for safeguarding PII.
- Only acquire and use PII as authorized.





# E-MAIL Safeguards To Protect PII



## Email Correspondence:

Subject line will be clearly marked “Privacy Act or FOUO”

Use DoD CAC Automated Information Systems (AIS) encryption and digital signature so that information, if compromised, is unusable by unauthorized individuals.

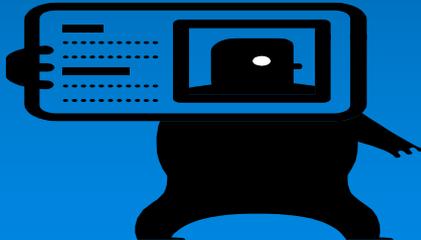




## WHY IS IT IMPORTANT TO SAFEGUARD PII?

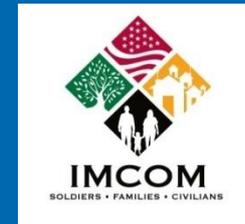


- Unauthorized recipients may fraudulently use the information (identity theft).
- Damage to the victim can affect their good name, credit, job opportunities, and could even result in criminal charges and arrest. Resolution is costly and time consuming.
- See Video on IMCOM PA Website for further information.
- As a Government employee you can personally suffer criminal or civil charges and penalties for failure to protect PII.





# COLLECTING PII



- If you collect it, you must protect it!!
- If in doubt, leave it out!!
- Do you really need the entire SSN or would the last 4 digits do?





## DOES PA/PII APPLY TO CONTRACTORS?



# YES!!

Employees of Government Contractors working for a Federal Agency are subject to the Privacy Act as far as working with Government information is concerned, and must comply with all of its provisions.





## WHO IS AUTHORIZED TO RECEIVE PII



- Congress, FOIA, Law Enforcement, DOD Employees with official need to know to perform official Government duties.
- Other disclosures may be permitted depending on the description of the record system. If unsure, do not release!





## PROPER DISPOSAL OF PII

- Disposal Methods May Include Burning, Melting, Shredding, Chemical Decomposition, Etc.



- Recycling Is Acceptable, **But** Only If The Documents Are Properly Protected While In The Destruction Bin, Protected In Transit And Destroyed By One Of The Above Destruction Methods.

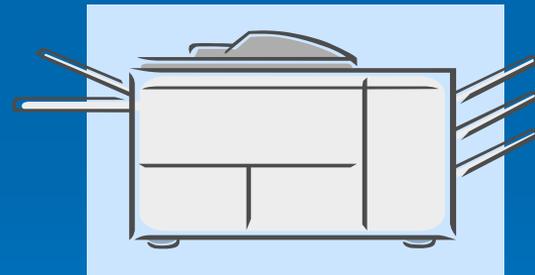




# PROPER DISPOSAL OF COMPUTER HARD DISK DRIVES



- Directorates, Units and Staff Offices are responsible for ensuring all computer hard drives are purged before reuse in a different environment, with a different classification level of data or with a different need-to-know authorization of users.
  
- Computer Hard Drives are on the following equipment:
  - Copiers
  - FAX Machines
  - Peripherals
  - Electronic Typewriters
  - Word Processing Systems
  
- Contact Network Enterprise Command (NEC) at [Benn.doim.ia.team@conus.army.mil](mailto:Benn.doim.ia.team@conus.army.mil) for approved methods of destruction of the hard drives.

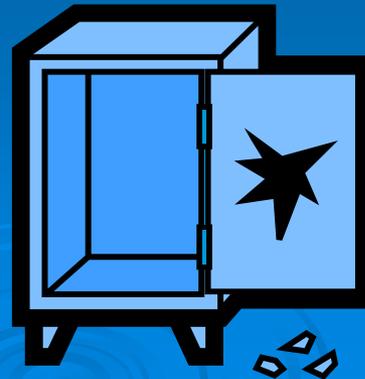




## WHAT IS A BREACH OF PII?



A breach of PII is the actual or possible loss of control, unauthorized disclosure or unauthorized access of personal information to persons other than those with an authorized “need-to-know” in order to perform official government duties.





## WHAT IMPACT DOES THE LOSS OF PII HAVE FOR DA?



- Can erode confidence in the government's ability to protect information
- Can impact our business practices
- Can lead to major legal action





## WHAT ARE THE MAJOR IMPLICATIONS FOR AFFECTED DA PERSONNEL?



- Can be embarrassing.
- Can cause emotional stress.
- Can lead to identity theft which can be costly to both the individual and the government.





## WHAT ARE THE MAJOR IMPLICATIONS FOR THE INDIVIDUAL(S) RESPONSIBLE FOR THE LOSS/COMPROMISE?



- Can result in disciplinary actions.
- Can result in civil or criminal actions being taken against the employee.
- Can result in costly fines and imprisonment.





## WHAT MUST YOU DO IF A BREACH OF PII OCCURS? (REPORTING PROCEDURES)



WITHIN ONE HOUR OF DISCOVERY THE PERSON DISCOVERING THE INCIDENT WILL:

- REPORT INCIDENTS WHETHER SUSPECTED OR CONFIRMED TO US-CERT.GOV BY FILLING OUT THE REPORT AT <http://www.us-cert.gov>
- NOTIFY THE ARMY LEADERSHIP AND FORT BENNING PRIVACY ACT OFFICE BY SENDING AN E-MAIL CONTAINING INFORMATION ON NEXT SLIDE TO:

<https://www.rmda.army.mil/privacy/foia-incidentreport1.asp>

[BENN.DHR.FOIA/ProjectOfficer@conus.army.mil](mailto:BENN.DHR.FOIA/ProjectOfficer@conus.army.mil)





## WHAT MUST YOU DO IF A BREACH OF PII OCCURS? (REPORTING PROCEDURES)



### COMMANDER'S CRITICAL INFORMATION REQUIREMENT FORMAT FOR PII REPORTING:

- ORGANIZATION IN WHICH PII BREACH OCCURRED
- TYPE OF INCIDENT
- DATE/TIMEGROUP OF THE INCIDENT
- LOCATION
- PERSONNEL INVOLVED
- SUMMARY OF INCIDENT
- REMARKS
- PUBLICITY
- OFFICIAL REPORTING
- POC



## WHAT YOU MUST DO IF A BREACH OF PII OCCURS? (REPORTING PROCEDURES)

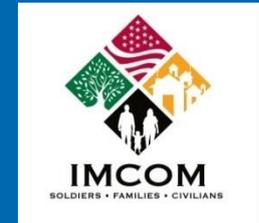


➤ THE DIRECTOR OR COMMANDER OF THE ORGANIZATION POSSESSING OR RESPONSIBLE FOR SAFEGUARDING THE PII AT THE TIME OF THE INCIDENT MUST NOTIFY THE AFFECTED INDIVIDUALS AS SOON AS POSSIBLE, **BUT NLT 10 DAYS AFTER THE BREACH/COMPROMISE IS DISCOVERED.**

➤ SAMPLE NOTIFICATION LETTERS ARE AVAILABLE AT:  
<https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf>

➤ A COPY OF THE LETTER WILL BE E-MAILED TO:  
[BENN.DHR.FOIA/PROJECTOFFICER@CONUS.ARMY.MIL](mailto:BENN.DHR.FOIA/PROJECTOFFICER@CONUS.ARMY.MIL)





# PII CONCLUSION - DO

- ONLY COLLECT PII THAT IS NECESSARY TO ACCOMPLISH AN OFFICIAL BUSINESS FUNCTION
- PROVIDE A PRIVACY ACT (PA) STATEMENT WHEN REQUESTING PA INFORMATION
- PII NOT CURRENTLY BEING WORKED WITH WILL BE SECURED IN A LOCKED CABINET



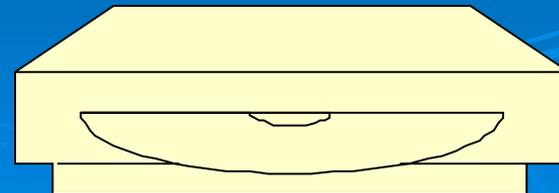
- MAINTAIN & APPLY ESTABLISHED SAFEGUARDING PROCEDURES
- ALLOW INDIVIDUALS TO REVIEW AND OBTAIN RECORDS ABOUT THEMSELVES UNLESS THE RECORDS ARE EXEMPT FROM MANDATORY DISCLOSURE

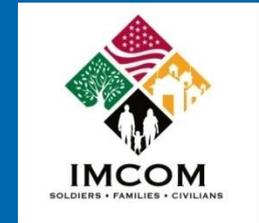


# PII CONCLUSION - DO NOT



- DO NOT COLLECT PII WITHOUT PROPER AUTHORIZATION
- DO NOT PLACE PII ON SHARED DRIVES, MULTI-ACCESS CALENDARS, OR THE INTRANET UNLESS ALL USERS HAVE A VALID NEED TO KNOW IN ORDER TO PERFORM OFFICIAL DUTIES
- DO NOT PLACE PII ON INTERNET PUBLIC FACING WEBSITES





## CERTIFICATE OF INITIAL/ANNUAL REFRESHER TRAINING

This is to certify that I have received initial/annual 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 incident to performing 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)

---

(Print Name)

---

(Date)

---

(DoD Component/Office)