



FOIA/PRIVACY ACT 101

*What you Need to Know about Safeguarding
Protected Personal Information (PPI)
and Personally Identifiable Information (PII)*

PURPOSE OF THIS TRAINING:



- *To define what is FOIA and the Privacy Act of 1974*
- *To focus on the importance of privacy and to ensure all OSD/JS personnel (military, civilian, contractor) are aware of the vital role that they must play in ensuring that PPI/PII is properly protected from unauthorized disclosure IAW FOIA and the Privacy Act of 1974.*

DEFINITIONS



- ***FOIA – Freedom of Information Act***
- ***PPI – Protected Personal Information***
- ***PII – Personally Identifiable Information***
- ***PPI/PII – Information which can be used to identify a person uniquely and reliably, including but not limited to name, SSN, address, telephone #, e-mail address, mother's maiden name***
- ***PPI and PII are interchangeable***

What's FOIA?



- *A statute that any person has the right to access to Federal agency records*
- *Unless those records (or portions of records) are protected from disclosure by any of the exemptions contained in the statute.*
- *There are **NINE** Exemptions that protect “exempt” information from public disclosure*

EXEMPTIONS



- *One – Classified (under an Executive Order)*
- *Two – Internal administrative matters*
- *Three – Other federal statutes, to include critical infrastructure security information (***NEW***)*
- *Four – Business information*
- *Five – Privileged information*
 - ✓ *Attorney-Work Product Privilege*
 - ✓ *Attorney-Client Privilege*
 - ✓ *Deliberative Process Privilege*
 - ✓ *Presidential Communications Privilege*
- *Six – Personal privacy*
 - ✓ *Personnel record*
 - ✓ *Medical file*
 - ✓ *Public interest vs. privacy*

EXEMPTIONS (Cont'd)



- **Seven – Confidential sources compiled for law enforcement purposes**
 - ✓ **7(A). Could reasonably be expected to interfere with enforcement proceedings**
 - ✓ **7(B). Would deprive a person of a right to a fair trial or an impartial adjudication**
 - ✓ **7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy**
 - ✓ **7(D). Could reasonably be expected to disclose the identity of a confidential source**
 - ✓ **7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions**
 - ✓ **7(F). Could reasonably be expected to endanger the life or physical safety of any individual**
- **Eight – Information that concerns the supervision of financial institutions, i.e., bank records**
- **Nine – Geological information on wells**

Privacy Act of 1974

Basic Policy Objectives



- *Protects information of individuals that is in a “system of records”*
- *To restrict disclosure of personally identifiable records maintained by Executive branch agencies*
- *To grant individuals increased rights of access to agency records maintained on themselves*
- *To grant individuals the right to seek amendment of agency records that are not accurate, relevant, timely, or complete*
- *To establish a code of “fair information practices” which regulates the collection, use, maintenance and disclosure of personally identifiable information*
- **NO disclosure without written consent**

EXEMPTIONS



There are **TWELVE** Exemptions under the Privacy Act:

- *(b)(1) Intra-agency disclosures – “need to know”*
- *(b)(2) Disclosure required by FOIA*
 - ✓ *FOIA request in hand*
 - ✓ *No discretionary disclosure if a FOIA exemption applies*
- *(b)(3) Routine Use*
 - ✓ *Listed in a published system of records notice*
 - ✓ *Disclosure compatible with the purpose of collection*
- *(b)(4) Bureau of Census*
- *(b)(5) For statistical research and reporting*
- *(b)(6) NARA (National Archives and Records Administration)*

EXEMPTIONS (Cont'd)



- *(b)(7) Written request by the head of a law enforcement agency within/under control of the US - for authorized law enforcement activity*
- *(b)(8) Compelling circumstances affecting health and safety*
- *(b)(9) Congress*
- *(b)(10) GAO (Government Accountability Office)*
- *(b)(11) Court Order*
- *(b)(12) Debt Collection Act*

Why You Need to Know About Privacy:



- *We are collection, maintaining, distributing and disposing of information about individuals--YOU!*
- *The law requires you to take precautions when collecting, maintaining, distributing and disposing of PPI/PII*
- *The Privacy Act of 1974 contains both civil and criminal penalties for non-compliance.*

OFFICE OF MANAGEMENT AND BUDGET



- *OMB issued a Memorandum dated May 22, 2006, entitled “Safeguarding Personally Identifiable Information,” which directed agencies to provide training to all employees on their responsibilities to safeguard personally identifying information*
- *OMB issued another Memorandum dated May 22, 2007, entitled “Safeguarding Against and Responding to the Breach of Personally Identifying Information”*
- *Both Memoranda require agencies to provide privacy training to all employees*

YOUR ROLE



- *Understand the importance of ensuring that PPI/PII is properly protected*
- *Get involved in identifying best practices for protecting PPI/PII*
- *Be aware of the consequences for non-compliance*

REQUIREMENTS



- *Establish rules of conduct for collecting, maintaining, distributing, and disposing of personal information*
- *Publish Privacy Act system of records notices in the Federal Register for all approved collections of privacy information*
- *Ensure that we collect only data that is authorized by law & that we share information only with those who have a need-to-know*
- *Establish and apply data safeguards to protect information from unauthorized disclosure*
- *Allow individuals to review records about themselves for completeness and accuracy & to amend any factual information that is in error*
- *Keep record of disclosures made outside of DoD to authorized “routine users” described in the system notice*

Examples of Personal Data Requiring Protection



- *Financial, credit and medical data*
- *Security clearance level*
- *Leave balances; types of leave used*
- *Home address & telephone numbers, personal e-mail address*
- *Social Security Number*
- *Mother's maiden name; other names used*
- *Drug test results & fact of participation in rehabilitation program*
- *Family data*
- *Religion, race, national origin*
- *Performance ratings*
- *Names of employees who hold government-issued travel cards*

THE LOSS OF PPI/PII



IMCOM
SOLDIERS • FAMILIES • CIVILIANS



- *Can be embarrassing & cause emotional distress*
- *Can lead to identity theft, which is costly to the individual and to the Government*
- *Can impact our business practices & result in actions being taken against an employee*
- *Can erode confidence in the Government's ability to protect information*

DEPSECDEF MEMORANDUM



- *On June 15, 2005, the DepSecDef issued a Memorandum entitled, “Notifying Individuals When Personal Information is Lost, Stolen, or Compromised.”*
 - ✓ *Requires DoD activities to notify individuals within 10 days after the loss or compromise of protected personal information is discovered*
- *Directs that notification advise individuals of:*
 - ✓ *(1) what specific data was involved;*
 - ✓ *(2) the circumstances surrounding the loss, theft, or compromise;*
 - ✓ *(3) what protective steps the individual can take in response*
- *See also 32 C.F.R. § 310.50*

ADDITIONAL BREACH NOTIFICATION PROCEDURES



- *Agencies must report all incidents involving PII to the U.S.-Computer Emergency Response Team (“US-CERT”) within ONE HOUR of discovery--32 C.F.R. § 310.50(1).*
- *DoD Components must report all incidents involving PII to the Senior Component Official for Privacy within 24 hours of discovering the breach--32 C.F.R. § 310.50.*
- *Senior Component Official for Privacy, or a designee, shall notify the Defense Privacy Office of the breach within 48 hours upon being notified of the breach--32 C.F.R. § 310.50(2).*
- *Submit report to the Defense Privacy Office detailing the specifics of the breach--32 C.F.R. § 310.50(2)(i) - (iv).*

COLLECTING PPI/PII



- *If you collect it--you must protect it!*
- *If in doubt, leave it out! Do you really need the entire SSN or will the last 4 digits serve as a second qualifying identifier?*
- *Moving from a paper process to an electronic process requires you to identify any breach risks*

THINK PRIVACY WHEN SAFEGUARDING PII



- *Need to address whether collection & maintenance of all the information that we collect is “relevant and necessary,” and whether we can maintain “timely and accurate” information.*
- *The CIO may need to conduct a Privacy Impact Assessment (“PIA”) of electronic system to identify vulnerabilities.*

BEST PRACTICES



- *“FOR OFFICIAL USE ONLY-PRIVACY SENSITIVE-Any misuse or unauthorized access may result in both civil and criminal penalties.”*
- *Any email messages that contain PII/PPI must contain the proper markings AND be ENCRYPTED!*
- *Any PII/PPI that is contained or maintained on “mobile” equipment (PDAs, memory sticks etc.) must be ENCRYPTED!*
- *Think PRIVACY:*
 - ✓ *when considering the PII that you store on your computer, memory stick, PDA, etc.*
 - ✓ *when you send/receive e-mails that contain PII--are these messages properly marked?*
 - ✓ *when you create documents--do you need to include the entire SSN?*
 - ✓ *when placing documents in public folders in Outlook and on public web sites.*
 - ✓ *when disposing of PII--use cross-cut shredding, if possible*

YOUR RESPONSIBILITIES



- *Do NOT collect personal data without authorization.*
- *Do NOT distribute or release personal information to other employees unless they have an official need-to-know.*
- *Do NOT be afraid to challenge anyone who asks to see PA information.*
- *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.*
- *Do NOT commingle information about different individuals in the same file.*
- *Do NOT transmit personal data without ensuring that it is properly marked.*
- *Do NOT use interoffice envelopes to mail Privacy data.*
- *Do NOT place privacy data on shared drives, multi-access calendars, the Intra or Internet that can be accessed by individuals who do not have an official need-to-know.*
- *Do NOT hesitate to offer recommendations on how to better manage Privacy data.*

PRIVACY/FOIA RESOURCES



- *Defense Privacy Office*
 - ✓ *www.defenselink.mil/privacy*
- *Department of Homeland Security's Privacy Office*
 - ✓ *www.dhs.gov*
- *DOD CIO*
 - ✓ *www.defenselink.mil/cio-nii*
- *FOIA*
 - ✓ *www.FOIA.gov*



Privacy Act Data Cover Sheet

To be used on
all documents
containing personal
information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

The enclosed document(s) may contain **personal** or **privileged** information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in **CIVIL** and **CRIMINAL** penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

Privacy Act Data Cover Sheet