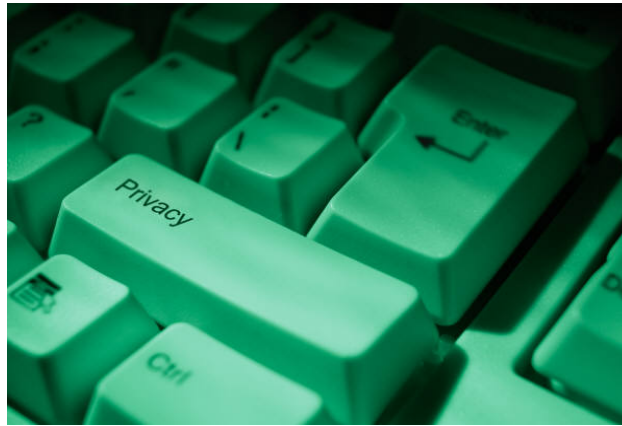


Protecting Personally Identifiable Information (PII) in an Electronic Age



**Environmental Information Symposium
Savannah, GA
December 5-7, 2006**

Is Your Personal Information Safe?



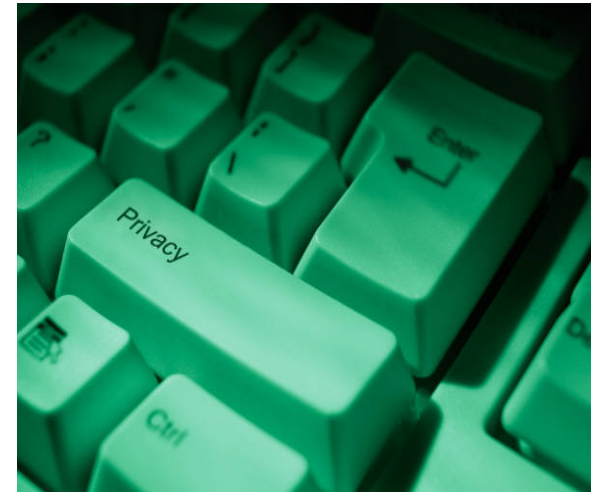
**Presenters: Judy Hutt, Don Huddleston,
Deborah Williams**

Office of Environmental Information

For Conference Purposes Only.

Purpose

- To provide an overview of PII, both sensitive & other types:
 - How does EPA identify PII?
 - How does technology impact PII?
 - What is EPA doing to safeguard PII?
 - How should one respond to PII Breaches (Agency & Individual)?
- To solicit your feedback & answer questions.



Privacy & E-Government Acts

- **Privacy Act of 1974**

- Establishes safeguards to protect records collected & maintained by the Federal Government on US citizens or lawfully admitted permanent residents.
- Pertains to information which is maintained in a system of records by an individual's name and/or other personal identifier.
- Does not include all “privacy” information.



Privacy & E-Government Acts

- Electronic Government Act 2002 (E-Gov Act)
 - Signed into law on Dec. 17, 2002
 - Became effective April 17, 2003
 - Established requirements for all agencies to:
 - **Conduct Privacy Act Assessments (PIAs) for electronic information systems and collections.**
 - **Post privacy notices on agency Websites used by the public**
 - **Translate privacy policies into standardized machine-readable format.**
 - **Designate a Privacy Official.**
 - **Report annually to OMB on compliance with Section 208.**



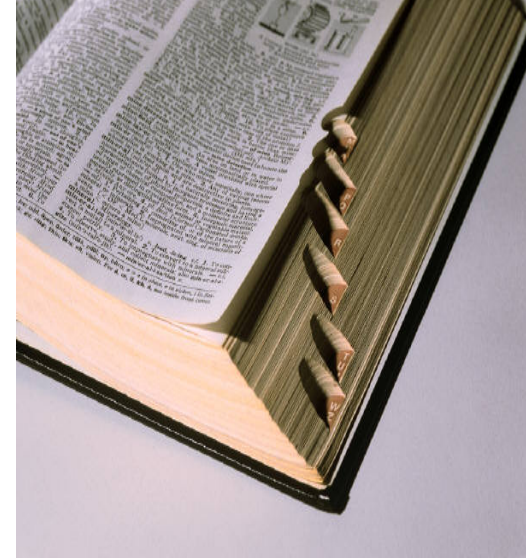
Massive breach of PII by Veterans' Administration

May 2006



Definitions

- **PII – Personally Identifiable Information**
 - Any information that can potentially be used to contact or locate an individual.
- **“Sensitive” PII**
 - SSN or comparable identifiers
 - Financial information associated with individuals
 - Medical information associated with individuals
- **Information in Identifiable Form (E-Gov Act 2002)**
 - Information in an IT system or online collection that: (1) directly identifies an individual (e.g. name, SSN, DOB,) or (2) in conjunction with other data elements allows for indirect identification (race, gender, demographic indicator).



EPA PII Taskforce

- Established June 2006
- Cross-Agency participation
- Protect PII from unauthorized access and disclosure focusing on technology, data, and policies
- Report to the Administrator in 180 days



PII Taskforce Accomplishments

- **Reviewed Agency system of records (SORs) notices**
 - Do they require modifications?
 - Is the PII collection still necessary?
- **Reviewing Agency forms that collect PII**
 - Do they require modifications?
 - Is the PII collection still necessary?
- **Reviewed technical controls & policies**
 - Are they consistent with National Institute of Standards and Technology (NIST) requirements?



PII Taskforce Next Steps

- Establish Agency baseline of all systems that collect PII
- Develop a risk matrix for PII elements
- Develop and conduct Privacy training
- Coordinate security and privacy compliance and oversight activities
- Ensure Privacy Act clauses are included in all Agency contracts



For Conference Purposes Only.

Protecting Privacy Policy A Team Effort



- Privacy Policy Committee
- Privacy Program Manual
- Telework Subcommittee
- Forms Review Committee
- Breach Subcommittee

Agency PII Policies

- EPA CIO Policy (Transmittal 06-011)
 - Issued August 23, 2006
 - **Purpose/Intent**
 - Senior Information Officer (SIO) approval required for off-site access to sensitive PII
 - Delegation of SIO approval not allowed
 - Prohibits local storage of sensitive PII
 - Identifies requirements for remotely accessing sensitive PII
 - **Encryption of “sensitive” PII**
 - Must occur prior to removal of sensitive PII
 - Requires Federal Information Processing Standards (FIPS) 140-2 validation



Agency PII Policies

- **Next Steps**

- **Mobile Device Encryption**

- **Criteria**

- 140-2 validation, ease of management, all portable devices, ease of support and recoverability of data, minimal impact of device being encrypted
 - File/Folder and Full disk encryption both being evaluated

- Gartner “Magic Quadrant Leaders” asked to respond
 - Complete product testing
 - Decide, purchase & implement



PII Taskforce Breach Subcommittee

- **OMB Memo:** “Recommendations for Identity Theft Related Data Breach Notification” (9/20/06) www.whitehouse.gov/omb/memoranda
 - **Issued guidance to federal agencies for planning and responding to data breaches which could result in identity theft.**



PII Taskforce Breach Subcommittee

- **OMB Guidance (con't):**

- Establish core management group**

- (1) Convene group;
 - (2) Engage in risk analysis,
 - (3) Produce risk-based tailored response.



- **OMB Guidance (con't):**

- **Actions Agencies can take:**

- Purchase Credit Monitoring Service
- Purchase Data Breach Analysis
- Notify Affected Individuals (Timing, Source, Contents, Method of Notification, Follow-on inquiries)



PII Taskforce Breach Subcommittee

- **What Can Individuals Do?**

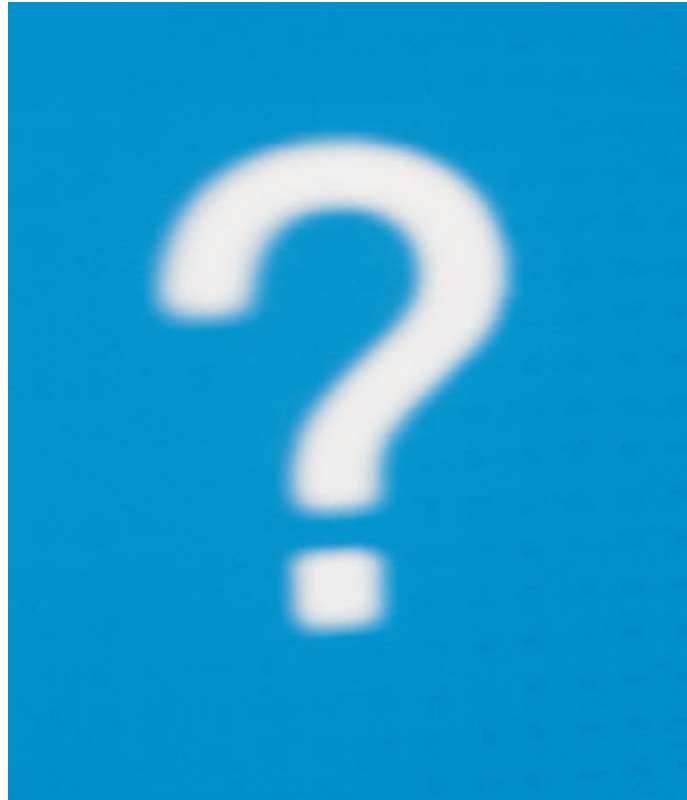
- **Actions Individuals Can Routinely Take:**

- Contact financial institutions to determine if accounts should be closed
 - Monitor financial account statements for suspicious or unusual activity
 - Request free credit report from www.annualcreditreport.com

PII Taskforce Breach Subcommittee

- **What Can Individuals Do?** (con't)
 - Place an initial fraud alert on credit report (option useful when breach includes info that can be used to open a new account, like SSNs)
 - Some states allow “credit freezes” which cuts off third party access to one’s credit report
 - Review resources at the FTC identity theft website, www.ftc.gov/idtheft

Questions?
Feedback? Concerns?



Contact Information

- For questions concerning the implementation of the Privacy Act & E-Government Act, contact Judy E. Hutt, Agency Privacy Act Officer, at (202) 566-1668 or Hutt.judy@epa.gov.
- For PII Breach & technology controls, contact Don Huddleston, at (202) 566-1462 or Huddleston.don@epa.gov.