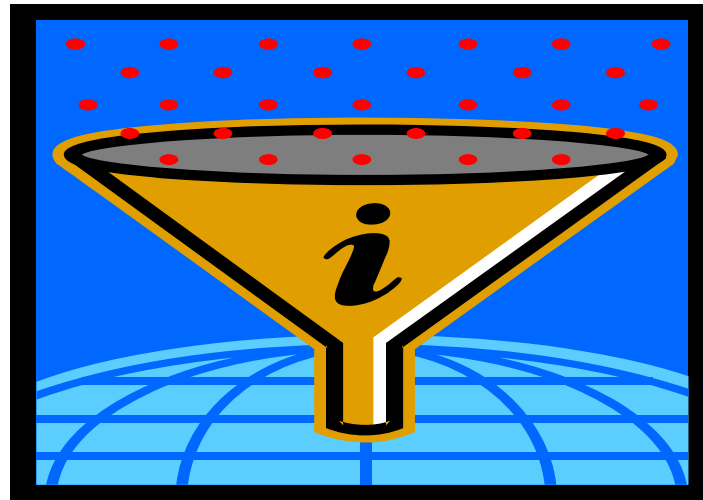


# Privacy: The Other Side of Transforming Information

(Protecting Individual's Privacy)



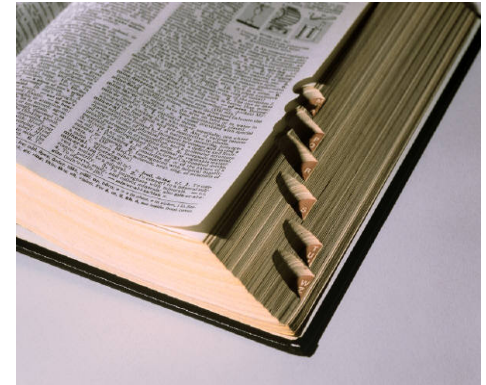
Environmental Information Symposium  
Wednesday, December 10, 2008  
Phoenix, Arizona

# Purpose

- Inform participants about the Agency's responsibilities for protecting the Personally Identifiable Information (PII) it collects, maintains, and/or disseminate.
- Discuss directives requiring Agency implementation.
- Discuss how the Agency's policies/procedures transform collected information into protected information.
- Discuss roles and responsibilities for key Privacy personnel.
- Discuss current initiatives in the Privacy Program.
- Inform participants about the Privacy Rules of Behavior and consequences for not complying.

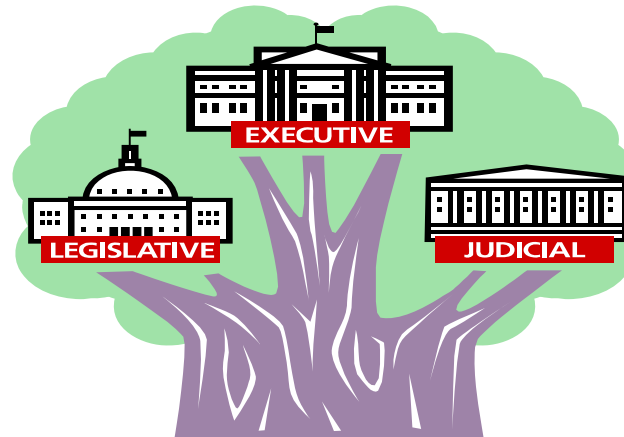
# Definitions

- **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).



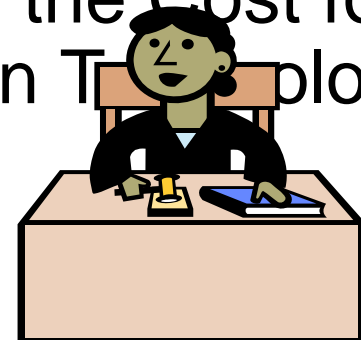
# Statutory Requirements Overview

- Privacy Act of 1974
- Electronic Government Act of 2002
- Federal Information Security Management Act (FISMA)



# Directives/Requirements

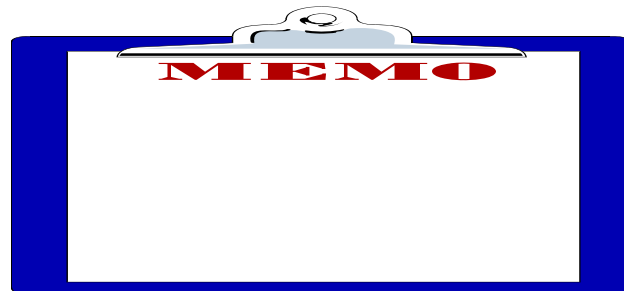
- OMB Memoranda
  - Safeguarding Personally Identifiable Information (M-06-15)
  - Protection of Sensitive Agency Information (M-06-16)
  - Reporting Incidents Involving PII and Information and Incorporating the Cost for Security in Agency Information Technology Investments (M-06-19)
  - IG Audit



**OMB M-07-16, “Safeguarding Against & Responding to the Breach of Personally Identifiable Information”**

Required Agencies to:

- Review current PII holdings.
- Publish a Routine Use Notice.
- Develop and publish a schedule for updating and reviewing of Agency PII holdings.
- Reduce use of social security numbers (SSNs).
- Eliminate unnecessary use of SSNs.
- Explore alternatives to Agency use of SSNs.
- Ensure understanding of privacy/PII responsibilities.



For Conference Purposes Only

# OMB M-07-19: “FY 2007 Reporting Instructions for FISMA and Agency Privacy Management”

- Breach notification policy.
- Implementation plan to eliminate unnecessary use of SSNs.
- Implementation plan on Agency review and reduction of PII holdings.
- Privacy Rules of Behavior.
- Consequences and corrective actions policy.

# Review of Privacy Program

## Office of Inspector General (OIG) Audit

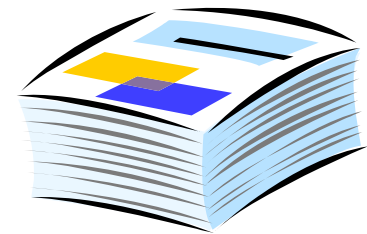
### Key Recommendations:

- Establish and track performance measures.
- Report progress to the Senior Agency Official for Privacy (SAOP).
- Update, implement, and communicate privacy policies and procedures.
- Develop roles and responsibilities for all key privacy personnel.
- Document consequences for not complying with policies and procedures.
- Develop sample cascading goals (PARs).
- Develop, maintain and publish a roster of key Agency personnel.
- Develop and implement processes for managing EPA privacy policies.
- Establish a monitoring and oversight process.



# Agency Response to OIG Recommendations

- Retreat held to identify remaining procedures required to fully implement the Privacy program.
  - Procedures to be developed.
    - SSN
    - Governance
    - Privacy Act Processing
    - On site reviews
- Key goals and activities posted on the **Privacy Intranet** site.
- Performance measures to be established.
- SAOP to be updated quarterly.



# Agency Policies

- Privacy Policy
- Breach Notification Procedure
- Incident Handling Procedure
- CIO Interim Policy 06-11
- Agency Network Security Policy



# Privacy Policy

- Established Agency National Privacy Program.
- Established roles and responsibilities for Agency staff:
  - employees
  - managers
  - contractors
  - grantees working on behalf of the Agency.
- Developed Breach Notification Procedure.
- Provides oversight responsibility for policies/procedures and requirements for:
  - administering
  - ensuring
  - complying



# Current Privacy Procedures

- Privacy Impact Assessments (PIAs)
- Privacy Act Statements (PAS)
- System of Record Notices (SORNs)
- Breach Notification
- Incident Handling



# Breach Notification Procedure

- Established a core management group (BNT).
- Established an evaluation group (BET).
- Established a central point of contact for all incidents (EPA Call Center).
- Identified other key personnel.

# Breach Notification Team (BNT)

- Chaired by the Senior Agency Official for Privacy (SAOP).
  - Comprised of senior management officials including the Office/Region in which the Breach occurred.
- Decides Agency course of action including notifying affected individuals.



For Conference Purposes Only

# Breach Evaluation Team (BET)

- Co-Chaired by OIC and OTOP.
- Developed Incident Handling Procedures
  - Determines the risk of harm to the affected individual and Agency.
  - Refers breaches of sensitive PII to the BNT, as appropriate.
- Prepares Fact Finding Report for BNT.
- Works with CSIRC to document the facts about the incident.



# EPA Call Center

- Triages incident.
- Inquires if caller is employee/contractor.
- Documents the reported incident.
- Records information from caller/ISO.
- Submits incident ticket to BET if PII is involved.



Transmitting/Transporting/Accessing  
Sensitive Personally Identifiable Information (PII)  
CIO Interim 06-11

- All sensitive data on personal computers and portable media and devices must be encrypted.
- All encryption technologies must conform to Federal Information Planning Standards (FIPS) 140-2.
- Remote access allowed only with two-factor authentication.
- All remote access and mobile devices must have automatic time out function requiring re-authentication after 30 minutes of inactivity.
- All requests for remote access must be approved by the SIO.



For Conference Purposes Only



# Procedures for Transmitting Sensitive PII

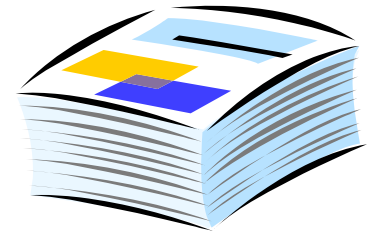


- Electronic Data

- Submit Request Form to remotely access electronic data (CIO 06-11).

- Non-Electronic Data

- Protect Non-digital (paper) files.



- Inner envelope should be marked “Contains Sensitive PII.”
- Outer envelope should be marked “To Be Opened by Addressee Only.”

# Key Privacy Personnel

## Senior Information Official (SIO)

- Designates the Liaison Privacy Official (LPO).
- Reviews and approves all requests for remote access to sensitive PII.
- Documents all approved downloads and/or local storage of sensitive PII.
- Ensures that all sensitive PII has been erased, returned, or destroyed within 90 days, or verify and authorize its continued use.
- Maintains a copy of all approved forms.

# **Key Privacy Personnel**

## **Information Security Officer (ISO)**

- Recommends LPO designation to SIO.
- Ensures completion of required training by users and compliance with requirements.
- Performs periodic reviews of existing databases to determine if PII data elements are still required.
- Approves initial determination for access to information.
- Ensures Privacy Impact Assessments are prepared for any system that collects PII.

# Key Privacy Personnel

## Liaison Privacy Official (LPO)

- Designated by SIO.
- Administers the day-to-day activities and responsibilities of privacy in their specific program and regional areas.
- Prepares privacy documentation for new and/or revised systems.
- Terminates systems when no longer maintained in accordance with proper destruction/transfer procedures.
- Ensures proper training for individuals in their area of responsibility, including monitoring on-line training for the employees.
- Attends annual training.

# All Employees

- Comply with the statutory provisions of the Privacy Act, E-Gov. Act, FISMA, Agency regulations, and program requirements.
- Report all incidents involving the security, loss misuse or unauthorized disclosure of PII regardless of form or format.
- Complete all required security awareness/privacy training.
- Complete and submit a request for remote access to sensitive PII to SIO.
- Place an unencrypted copy of the files that contain sensitive PII on the EPA computer network in the F:USERNAME directory.
- Do not download and/or locally store sensitive PII on a privately-owned hard drive (unless specifically authorized in writing by SIO).
- Destroy sensitive PII and ensure sanitation of digital media when it is no longer needed after 90 days.



For Conference Purposes Only



# Current Initiatives in the Privacy Arena

- EPA Smart Cards – (HSPD -12).
- PII Data Call.
- Review flexi-place contract to ensure adequacy of PII protection.
- Include Privacy Act clauses in Agency contracts.
- Develop Agency-wide general privacy training for all employees.
  - Provide specified training for:
    - HR employees
    - Contractors
    - LPOs

# Proactive Actions

- Work with Web managers, ISOs and SAs to ensure PII data does not reside on Web pages, servers, etc.
- Require new hires to complete security training immediately after coming on board.
- Work with LPO and ISO in the initial stages of developing a new investment that collects information.



# Rules of Behavior/Consequences

- Employees, managers, and supervisors must ensure that staff is properly trained.
- Report any suspected/confirmed breaches of information.
- Sample PARs for key personnel developed and posted to the Privacy Intranet site.
- Posted on the intranet site at:  
[http://intranet.epa.gov/rules\\_of\\_conduct\\_htm](http://intranet.epa.gov/rules_of_conduct_htm).

# Privacy Resources

- For policies, procedures, points of contact, upcoming meetings, etc. visit the Privacy Intranet Site at: <http://intranet.epa.gov/privacy>.
- External resources and policies visit the Privacy Internet Site at: [www.epa.gov/privacy](http://www.epa.gov/privacy).
- Agency Privacy personnel:
  - Senior Agency Official for Privacy (Molly O'Neill)
  - Chief Privacy Officer (Andrew Battin)
  - Agency Privacy Act Officer (Judy Hutt)
  - LPOs (See [www.epa.gov/privacy](http://www.epa.gov/privacy) for listing.)



# Questions



Questions regarding implementing Privacy requirements within the program and regional offices should be addressed to the LPOs at: [http://intranet.epa.gov/privacy/For\\_LPOs.htm](http://intranet.epa.gov/privacy/For_LPOs.htm)

Questions regarding how the Agency is implementing the National Privacy Program should be addressed to the Agency's Privacy Act Officer, Judy E. Hutt at: [hutt.judy@epa.gov](mailto:hutt.judy@epa.gov) or (202) 566-1668.