DEFENSE PRIVACY OFFICE

MITRE Technical Exchange Meeting

Turning the Corner:
Future Directions in Government Privacy

Presented by

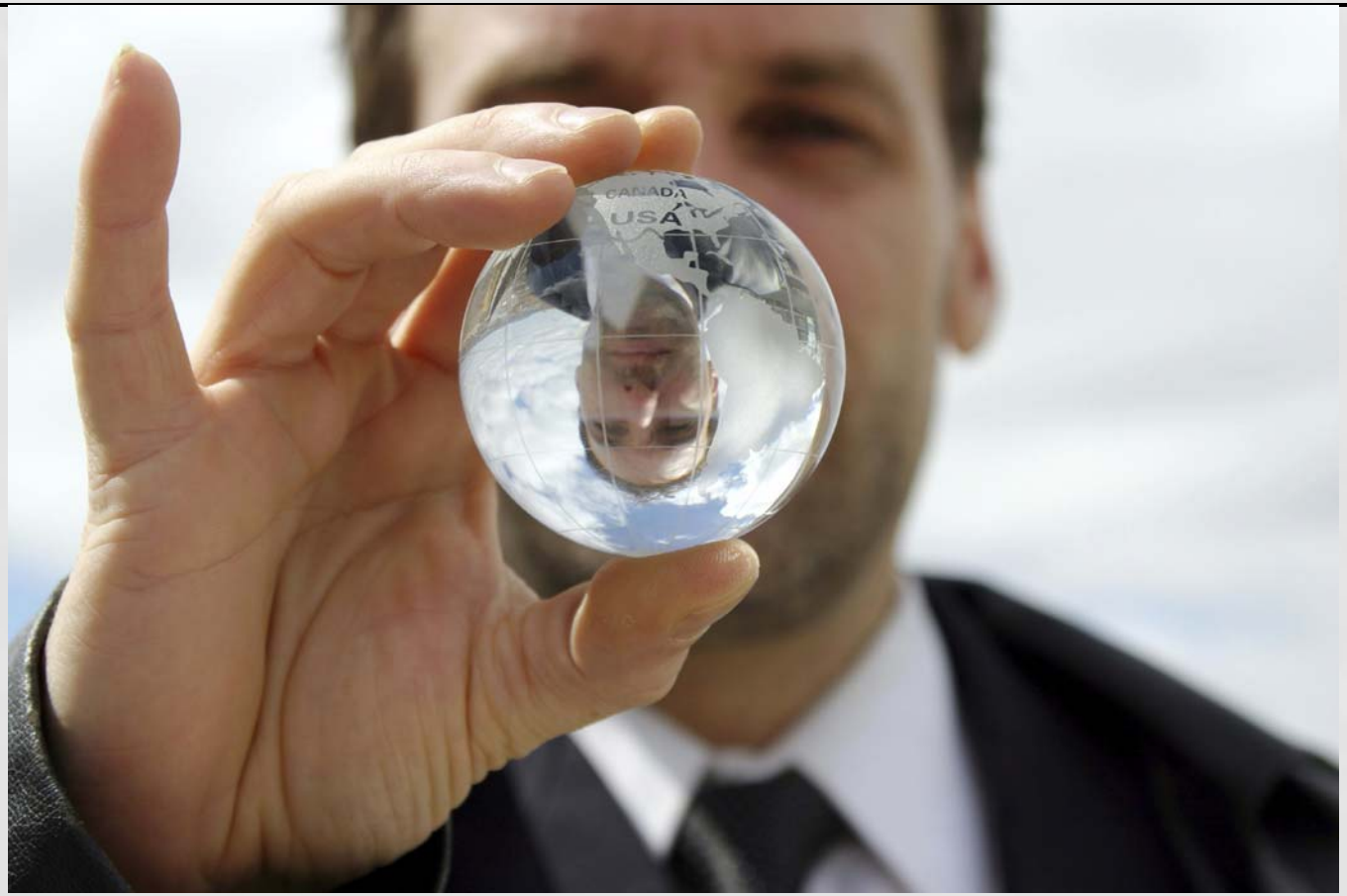
Samuel P. Jenkins, Director
Defense Privacy Office

May 18, 2009

Defense Privacy Office (DPO)

- Primary Responsibilities
  - DoD 5400.11-R, “DoD Privacy Program”, May 14, 2007
  - Privacy Act of 1974
  - OMB Circular A-130
  - Computer Matching Agreements
  - Systems of Records Notices (SORNs)
  - Applicability to Components

What's Around the Corner for DPO?



Review and Improve the Management of Privacy Act Systems of Records

- Based on law from 1974
- Emerging technology advancements
- Transition from “Paper Based” systems to “Electronic” collections of information
- Free flow of information within and between organizations
- Global information sharing
- Striking the balance between our needs for information and the individual's right to privacy

Review and Improve the Management of Privacy Act Systems of Records

- Each agency shall conduct a thorough review of its systems of records, system of records notices, and routine uses in accordance with the criteria and guidance established
- The goal is to focus agency resources on the most probable areas of out-of-date information, so that reviews will have the maximum impact in ensuring that system of records notices remain accurate and complete

Review and Improve the Management of Privacy Act Systems of Records

- Information maintained about individuals must be relevant and necessary
  - The Privacy Act limits agencies to maintaining "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished…"
  - Information that was relevant and necessary when a system of records was first established may, over time, cease to be relevant or necessary
  - If your agency determines that any information about individuals in a system of records or that the entire system of records is no longer relevant and necessary the agency should:
    - Revise or rescind the system notice, or
    - Expunge the records (or system of records) per procedures outlined in the Privacy Act Notice and prescribed record retention schedule

Review and Improve the Management of Privacy Act Systems of Records

- Privacy Act records must be protected by appropriate safeguards
  - Agencies must ensure the information's security and confidentiality.
  - Each agency shall review its systems of records to ensure that the safeguards in place are appropriate to the types of records and the level of security required
  - The Paperwork Reduction Act requires agencies to "implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency" and "identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency."

Review and Improve the Management of Privacy Act Systems of Records

- Routine Uses must meet the “compatibility” standard
  - The Privacy Act authorizes agencies to disclose information about individuals under a "routine use". A routine use is defined as a disclosure of a record outside of the agency for a use that is compatible with the purpose for which the information was collected
  - Each agency shall review its "routine uses" to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected
  - If an agency determines that the system of records notice does not accurately and completely describe the routine uses, the agency should revise the notice accordingly

Review and Improve the Management of Privacy Act Systems of Records

- Agencies must keep an accounting of disclosures and make it available
  - The Privacy Act requires agencies to "keep an accurate accounting" regarding "each disclosure of a record to any person or to another agency," and to retain the accounting for at least five years or the life of the record, whichever is longer
  - All disclosures under 5 U.S.C. § 552a(b) (except those made within the agency on a **need-to-know** basis or required by the **FOIA**) must be accounted for, including those made under routine uses, and those made pursuant to requests from law enforcement agencies (even though the latter may be exempt from disclosures to the subject individual)
  - Agencies must be able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to requests in a timely fashion

Review and Improve the Management of Privacy Act Systems of Records

- Systems of records should not be inappropriately combined
  - Groups of records that have different purposes, routine uses, or security requirements, or those that are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security. An agency should identify instances where a system of records includes groups of records which, because of their different purposes, routine uses, or security requirements, should not be combined into a common system of records but instead be maintained and managed as separate systems of records
  - Records that have the same purpose, routine uses, security requirements, and other attributes, and that are regularly accessed by the same categories of members across the agency should be evaluated for the appropriateness of combining multiple systems into an agency-wide system of records

Ensure Notices Describing Systems of Records are Up-To-Date, Accurate and Complete

- Transparency
  - In order to exercise their rights, individuals must have access to an up-to-date notice of what types of information are maintained and for what reasons.
  - Each agency shall conduct a review of its systems of records notices to ensure that they are up-to-date, to conform with any necessary changes identified during the review
  - The goal is to provide a notice helpful to someone who might be a subject of the records.
    - The reviewer should ask, "If this system of records contained information about my friends or family, would this notice allow them to understand what type of records are kept, who uses them, and why?"

Identify Any Unpublished Systems of Records

- DITPR – SORN status disconnect
  - In passing the Privacy Act, Congress made a strong policy statement that in order to ensure fairness, there shall be no recordkeeping systems whose existence is kept secret. Further, each agency shall review its operations to identify any *de facto* systems of records for which no system of records notice has been published
  - Agencies shall implement appropriate measures (e.g., training) to ensure that systems of records are not inadvertently established, but instead are established in accordance with the notice and other requirements of the Privacy Act

CURRENT ISSUES

- Information Sharing Environment (ISE)
- DNA
- Biometrics
- Role based Access to Systems and Data
- Training and Outreach
- Compliance Reporting