System of Records Notices and Privacy Impact Assessments

Kellie Robinson
Department of State

Cindy Allard
Defense Privacy, Civil Liberties and Transparency Division

Objective

- Provide an understanding of where privacy compliance is rooted
- Describe the fundamentals of the Privacy Act and E-Government Act compliance artifacts
  - System of Records Notices (SORN)
  - Privacy Impact Assessments (PIA)

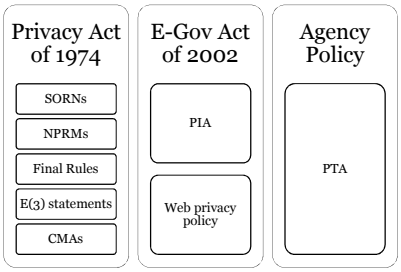
Privacy Compliance Process Model

4

Privacy Act v. Privacy Policy Compliance

– Two privacy analytical frameworks.
– Privacy Act: 1974
  – Goal: Access, redress, correction of government records
  – Goal: Appropriate SHARING of government records
  – Access: Similar to FOIA, except applies to records requested about yourself, rather than others
– E-Government Act: 2002
  – Beginning of Privacy POLICY framework
  – Protection of PII
  – Analyze the privacy risks of IT assets

Compliance artifacts



The Privacy Act of 1974

- The Privacy Act speaks to records maintained in a "system of records" that are retrieved by an individual's name and/or personal identifier.
- Each Executive Branch federal agency has a responsibility for identifying all records that contain personally identifiable information that are retrieved by an individual's name and/or personal identifier.

Policy Objectives of the Privacy Act

- To restrict disclosure of personally identifiable records maintained by the agencies
- To grant individuals an increased right of access and a right of amendment of records
- To establish a "code of fair information practices" that regulates the collection, maintenance, use and disclosure of personally identifiable records
- To grant individuals private rights of action for agency violations of the Act

Finding PA-covered Records

- Identify what kinds of records you are maintaining that are retrieved by a name and/or personal identifier
- Very important - Build a relationship with program managers so you can understand their needs/wants and translate them into a systems notice

What is PA "Record"?

- "Record" means
  - Any item, collection, or grouping of information
  - About an individual
  - That is maintained by an agency,
    - Including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph

Records

- Three prong test for Records:
  - Must be about the individual
  - Must identify the individual
  - Must be maintained by the agency

System of Records

- Three prong test for System of Records:
- "System of records" means:
  - A group of any records
  - Under the control of any agency
  - From which information is **retrieved** by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual

Retrievability

- Standard: Actual Retrieval
  - OMB Guidelines:
    - A system of records exists if:
    - (1) There is an indexing or retrieval capability using identifying particulars built into the system AND
    - (2) the agency does, in fact, retrieve records about individuals by reference to some personal identifier
  - Confirmed by case law:
    - *Henke v. U.S. Department of Commerce*, 83 F. 3d 1453 (D.C. Cir. 1996)
      - "Capability to retrieve, alone, is insufficient."

System of Records (cont'd)

- Why is this definition so important?
  - Most of the rights and requirements of the Privacy Act depend on whether this definition is met.
    - For ex. Wrongful disclosure suits, access and amendment rights
- Notice Requirements:
  - Must publish a system of records notice **(SORN)** in the Federal Register (5 U.S.C. § 552a(e)(4))

Why a SORN?

- It's the foundation of our Privacy programs
- It's transparency – enabling people to know what kinds of information we are collecting and on whom
- It's your tool to answer Privacy Act questions
- It's rulemaking
- It's a blueprint that describes our business practice
- It's the authority for sharing information with others
- It's something that we update regularly to reflect changes in business practices

What does a SORN look like?

- System Name: important to have one that is easily understandable – avoid acronyms
- System Identifier: A number that identifies it (i.e., DHS/ALL-009 DOE 1, DWHS P43, etc)
- Classification: OMB Circular A-108 requires a classification level for the records being maintained

SORN Sections

- System Location: The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider
- System Manager(s): Identifies the responsible official for the system. Sometimes you will list a Policy Official at a high level and a records holder at a local level.

SORN Sections

- Authority for Maintenance of the System: Identifies the basis for collecting the information (i.e., specific statute, regulation, executive order)
- Purpose(s) of the System: Addresses why you are collecting the information (i.e., To evaluate…; to nominate…; etc.) and identifies any internal agency sharing of the information and for what purpose

SORN Sections

- Categories of Individuals Covered by the System: Identifies who we are collecting information on (i.e., civilian employees, military members, contractor employees, dependents)
- Categories of Records in the System: Defines the kinds of records you are maintaining, such as "Personal information that includes name, address, etc.; "

SORN Sections

- Record Source Categories: Identifies where the information is obtained (i.e., individual; personnel file; etc.)
- Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses:
  - Identifies who **outside the agency** you can share the information with and for what purpose
  - These are discretionary; Routine Uses do not REQUIRE sharing.
  - Usually require a written request, written response, and a disclosure accounting record

SORN Sections

- Storage: How is the information stored? Electronic database? Paper records? Microfiche?
- Retrieval: This is what makes it a PA system of records – must be retrieved by a name and/or personal identifier.

SORN Sections

- Retention and Disposal: Describes how long the records will be kept and how they will be disposed of (i.e., records are maintained for 6 years and then shredded; permanent – retired to NARA after 42 years)
- Safeguards: A description of the administrative, technical, and physical safeguards to which the system is subject

SORN Sections

- Record Access Procedure: Tells the public where to write and what to provide to identify themselves so their records can be made available to them
- Contesting Record Procedures: Identifies where an individual may contest the content of any record pertaining to him or her in the system. Usually includes the Code of Federal Regulations citation
- Notification Procedure: Tells the public who to contact and what to provide to determine if records are held on them

SORN Sections

- Exemptions Promulgated for the System: Identifies what information may be exempt from disclosure and references that a rule establishing the exemption has been published in the Federal Register. In most instances, it states NONE.
- History: The citation to the last full publication of the notice in the Federal Register and any subsequent notices of revision

The E-Government Act of 2002

Title II; Section 208

- Ensures sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government
- Emphasizes the importance of the "development of a comprehensive framework to protect the government's information, operations, and assets"
- Requires agencies to conduct PIAs

The E-Government Act of 2002

PIA requirements

- Requires agencies to conduct PIAs *before*:
  - Developing or procuring new **IT** that collects, maintains, or disseminations personal information
  - Any new collections (regardless of IT form):
    - Collected, maintained or disseminated by IT; or
    - From 10 or more members of the public (PRA standard)

The E-Government Act of 2002

PIA requirements

- Basic PIA requirements from Section 208:
  - What information is collected;
  - Why the information is collected;
  - Intended use of the information;
  - With whom the information will be shared;
  - Notice or opportunities for consent is provided;
  - How information will be secured; and
  - Whether a system of records has been created.
- Agencies can opt to expand

OMB M-03-22

Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- Conduct PIAs for electronic information systems and collections and, in general, make them publicly available
- Post privacy policies on agency websites used by the public
- Translate privacy policies into a standardized machine-readable format
- Report annually to OMB on compliance with section 208 of the Act

OMB M-03-22

Examples of Privacy Risks
- Converting a system from paper based to electronic
- Changing anonymous data into identifiable form
- When new technologies change the way data is managed in a system
- Significant merging of data
- New ways members of the public can access data (password, biometric, digital certificate)
- Incorporation of commercial data sources
- New interagency uses
- Alteration in the character of the data (addition of health or financial data)

Privacy Impact Assessments

- A successful PIA should accomplish two goals:
  - Determine the **risks and effects**; and
  - Evaluate **protections** and alternative processes to **mitigate potential privacy risks**.

Privacy Impact Assessments

- A PIA is an analysis of how information is handled that:
  1. Ensures conformance with applicable legal, regulatory, and policy requirements for privacy;
  2. Reveals potential privacy vulnerabilities and effects; and,
  3. Examines and evaluates protections and alternative processes.

Conduct a PIA when…

- Developing or procuring any new technologies or systems that handle or collect personally identifiable information.
- Developing system revisions that contribute to new privacy risks.
- Issuing a new or updated rulemaking that entails the collection of personally identifiable information.
  - Even if a component has specific legal authority to collect certain information or build a certain program or system, a PIA is required.

PIA Process

- Iterative process with program, legal counsel, IT and Privacy Office collaborating
- Start at the beginning of a new program and build in privacy

Privacy Act v. E-Government Act

- Both contribute to transparency and accuracy of agency information
- Privacy Act generates private rights of action
- E-Government Act tailored to IT, but can be expanded
- "Individual"
  - Under Privacy Act, "Individual" limited to U.S. citizens or LPRs, and cannot legally be expanded
  - Agencies can expand E-Gov definition

Bottom Line: SORNs v. PIAs

- SORNs are a legal requirement to provide notice to individuals about how to access, correct, and amend their records
- PIAs are legally required risk-based evaluations of an agency's IT assets that maintain PII.
- Both are required to be posted on an Agency's website.

Questions about Privacy Compliance?