Privacy for Security Professionals

March 13, 2008

Sally L. Wallace, CISSP

ADAS for Privacy and Records Management

Discussion Topics

- **Key Privacy Laws/Guidelines**
- **Privacy Impact Assessments**
- **System of Records Notice**
- **Web/COPPA**
- **Fair Information Principles**

Key Privacy Laws

- **Privacy Act of 1974**
- **E-Government Act of 2002**
- **Children's Online Privacy Protection Act (COPPA), 1998**
- **Health Insurance Portability and Accountability Act (HIPAA), 1996**
- **Gramm-Leach Bliley Act (GLBA), 1998**
- **Freedom of Information Act (FOIA), 1966 and amended**

Key OMB Privacy Guidelines

- **M-07-16, dtd May 22, 2007, Safeguarding against and Responding to the Breach of PII**
- **M-06-15 dtd May 26, 2006 regarding Safeguarding PII**
- **M-05-08 dtd February 11, 2005 regarding Senor Agency Officials for Privacy**
- **M-03-22 dtd September 26, 2003 – Guidance for Implementing Privacy Provisions of E-Gov Act of 2002**
- **M-01-05 dtd December 20, 2000 regarding computer matching**

Privacy Impact Assessments (PIAs)

- Required when developing/procuring IT systems that collect, maintain or disseminate individually identifiable information.
- Required when initiating new electronic collection of information in identifiable form.
- Required where a system change creates new privacy risks.
- Tool for ensuring that privacy issues are properly addressed throughout the life cycle of each agency information system.

Privacy Impact Assessments (PIAs)

- To be initiated in early stages of development, when requirements are being analyzed.
- Must reflect current information collection practices, and accurately describe the data, uses, and handling of the information
- Identify the risks and adverse effects of collecting, maintaining and disseminating personal information in electronic information systems
- PIA's are sent to OMB and required to be made publicly available.

Systems of Records Notices (SORNs)

- **Required by the Privacy Act**
- **SORNs are required for systems that store data that the agency retrieves by the individuals' name or other identifiers (eg social security number or date of birth)**
- **Applies to records created and maintained by the agency or anyone acting on the agency's behalf (contractors or other Federal agencies).**
- **Before an agency operates a system of records, it must publish a notice in the Federal Register.**
- **Any "significant" changes to systems require a notice in the Federal Register.**
- **SORNs must also be reviewed by OMB and key members of the Privacy Act oversight committees.**

Special Web Issues

- **Collecting Information from a Web Page:**
  - **E-Gov Act of 2002 requires Privacy policies in both human and machine readable format on web pages that collect data.**
  - **Forms collecting data from public require OMB approval.**
  - **Children's Online Privacy Protection Act (COPPA) applies to online collection of personal information from children under 13.**

Fair Information Principles

- **Openness**
- **Individual Participation**
- **Limited Collection**
- **Limited Retention**
- **Data Quality**
- **Limited Internal Use**
- **Disclosure**
- **Security**
- **Accountability**
- **Challenging Compliance**

Eliminate Unnecessary Use of PII

- **Many Privacy violations are caused by exposure of SSN and other private information to 3rd parties via misrouted mail, misrouted faxes, etc.**
- **Agencies had to develop plans to eliminate the unnecessary use of SSNs, and to reduce holdings of PII as per OMB guidance.**
- **SSN's should be eliminated from print and display wherever possible.**
- **SSN's should be collected once, if needed, and then secured.**
- **Unique identifiers are preferable to SSNs.**
- **Executive order mandating use of SSN as an identifier is being rescinded.**