Privacy Policy Implementation and HSPD-12

OMB Public Meeting
Washington DC, January 19, 2005

John T. Sabo
Computer Associates
john.t.sabo@ca.com

Privacy and HSPD-12

1) ...it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government ....

6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

Privacy Act Requirements

- Identify each system of records and publish notice
- Review content to ensure collection and maintenance are necessary and relevant to law or executive order
- Inform individuals: purpose collected, rights, benefits, obligations
- Maintain accounting of all disclosures of information except Freedom of Information Act and agency “need to know” staff
- Assure records are accurate, relevant, timely, complete
- Permit individuals access and amendment of records
- Provide reasonable safeguards regarding disclosures and protections against security and integrity threats

Canadian Standards Association's Model Code for the Protection of Personal Information

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

One example of well-recognized privacy principles and practices

Privacy Impact Assessments

- M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Section 208 of the E-Government Act of 2002 - privacy impact assessments for electronic information systems and collections addresses:
  - **what information is to be collected**
  - **why the information is being collected**
  - **intended use of the information**
  - **with whom the information will be shared**
  - **what opportunities individuals have to decline to provide information**
  - **how the information will be secured**
  - **whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a**
- Not Addressed:
  - **Individual access**
  - **Amendment of records**
  - **Maintain accounting of all disclosures of information**
  - **Assure records are accurate, relevant, timely, complete**

ISPAB Report

- Information Security and Privacy Advisory Board September 2002 Report (csrc.nist.gov/ispab)
  - networked, distributed systems and migration toward e-Government services place greater demands on the government's privacy policies and systems
  - With additional authorities and the increased use of information systems for homeland security, fundamental government privacy policy and management issues deserve accelerated attention
  - changes in technology...the accelerated interaction of networked information systems...the extended, routine exchange of data among Federal and non-Federal government and non-government systems mandate immediate and serious attention to Federal government's data privacy policies and operational controls
  - recommended a structured approach to dealing with these issues

Four Privacy References in FIPS-201 v.1.0 Draft

- Section 3.1 Functional Objectives
  - "Protect the privacy of the card holder" (as threat mitigation and to guide standard development)
- Section 6.1 PIV Card Authentication Mechanisms
  - "For privacy reasons contactless use of PINs and biometrics is not supported..."
- Annex A - Table A-4, Standards for Validated Components
  - ..."FIPS 201 validation may involve some minors tests for conformance to the issuing agency's policies, such as the verification of credentials in the PIV card for conformance to the issuing agency's privacy policy."
- Annex A Section A.2.4 Validation Maintenance
  - "Whenever there is a change in the card issuance system and card design, the issuing agency shall re-validate the PIV card issuance system to ensure that privacy requirements are still met."

Issue: Developing Companion Policy Guidance on Privacy Requirements

- HSPD-12 is clear about govenment's privacy responsibilities
  - ***6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans***
- Leadership needed on companion policy guidance on privacy
  - differences among agencies on privacy policies for identity information can work against standard envisioned by HSPD-12
  - Privacy policies in place before FIPS 201deployments
- Possible annex to FIPS 201 or separate NIST or OMB guidance
- Focus on the privacy policy and privacy process management aspects of implementing PIV systems

Recommendations

- Address privacy management responsibilities with the same diligence as security
- Make this a focused project, with OMB/NIST leadership and a clear set of deliverables coincident with HSPD-12 timeframes
- Use NIST's standards development process
- Consider a Special Publication on agency HSPD-12 privacy management, with both agency and vendor input and assistance

Recommendations

- Use existing bodies and expertise, including industry and government efforts
  - Information Security and Privacy Advisory Board (ISPAB)
  - Industry efforts such as those of the International Security Trust and Privacy Alliance's (ISTPA) Privacy Framework projects
  - the emerging international PETTEP (Privacy Enhancing Tools and Technology Evaluation Project)
  - Enhanced privacy profile under the CIO Council's Federal Enterprise Architecture (FEA)
- Information privacy policy and standards development can benefit from industry expertise in compliance management, e.g. Sarbanes-Oxley compliance solutions

For more information:

john.t.sabo@ca.com
www.ca.com/federal
www.istpa.org
csrc.nist.gov/ispab