Better Privacy Through Identity Management:

Report of the Identity Theft Prevention and Identity Management Standards Panel (IDSP)

Presented By:
Jim McCabe
Director, Consumer Relations and IDSP
American National Standards Institute

The Privacy Symposium
August 20, 2008

ANSI
American National Standards Institute

Topics to be covered

1. What is IDSP?
2. Overview of ANSI-BBB IDSP Report
3. Current IDSP Activities of Interest
4. Your Questions . . .

What is IDSP?

- Cross-sector coordinating body whose objective is to facilitate the development, promulgation and use of standards and guidelines to combat ID theft and fraud
  - Identify existing standards, guidelines and best practices
  - Analyze gaps, need for new standards, leading to improvements
  - Make recommendations widely available to businesses, government, consumers

ANSI-BBB IDSP – Phase 1

- A 16 month effort – September 13, 2006 to January 31, 2008
- Co-administered by the American National Standards Institute (ANSI) and the Better Business Bureau (BBB)
- 165 representatives from 78 organizations
  - Founding Partners: AT&T; ChoicePoint; Citi; Dell Inc.; Intersections, Inc.; Microsoft; Staples, Inc.; TransUnion; and Visa Inc.
- 3 Working Groups explored life cycle of identity issues
  - Standards relating to issuance of identity documents by government and commercial entities
  - Standards relating to acceptance and exchange of identity information
  - Standards relating to ongoing maintenance and management of identity information

ANSI-BBB IDSP Report (Jan 31, 2008)

- *Summary*
  - Excerpt from *Volume I: Findings and Recommendations*
- *Volume I: Findings and Recommendations*
  - Findings and recommendations for areas needing new or updated standards, guidelines, best practices or compliance systems
- *Volume II: Standards Inventory*
  - Catalog of existing standards, guidelines, best practices and compliance systems

- Available for free download at www.ansi.org/idsp along with replay of industry analysts webinar

Volume I: Findings and Recommendations

- Enhance security of identity issuance processes to facilitate greater interoperability between gov’t and commercial sectors
- Improve integrity of identity credentials
- Strengthen best practices for authentication
- Augment data security management best practices, e.g., on the use and storage of Social Security numbers
- Create uniform guidance for organizations on data breach notification and remediation
- Increase consumer understanding of ID theft preventative strategies, including benefits and limitations of security freezes

Volume II: Standards Inventory

- Catalogues . . .
  - Existing Standards, Guidelines and Best Practices
    - PRIVATE AND PUBLIC SECTOR
  - Laws / Regulations
  - Proposed Legislation
  - White Papers
  - Conformity Assessment Programs
  - Glossaries of Identity Terms
  - Research Studies / Reports

Standards Inventory - Sample Entry

Developer/ Source	Designation	Title	Description/Scope	Relevance to IDSP Working Group
ISO/IEC	ISO/IEC 27002:2005	Information technology - Security techniques - Code of practice for information security management	■ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: ●security policy; ●organization of information security; ●asset management; ●human resources security; ●physical and environmental security; ●communications and operations management; ●access control; ●information systems acquisition, development and maintenance; ●information security incident management; ●business continuity management; ●compliance.	3

Issuance of Identity Credentials

Working Group 1 – Findings and Recommendations

Topics covered

- Enhance Security of the Issuance Process
- Augment Private Sector Commercial Issuance Processes
- Improve the Integrity of Identity Credentials

Issuance of Identity Credentials

Enhance Security of Issuance Process

Recommendation #1

- *Issue standards for birth certificates and Social Security cards*
  - National Ctr. for Health Statistics and Social Security Admin. should do so under Intelligence Reform and Terrorism Prevention Act of 2004
- *Improve communication / cooperation between government agencies and private sector*
  - National Assn. for Public Health Statistics & Information Systems should expand to government agencies use of Electronic Verification of Vital Events system

Issuance of Identity Credentials

Enhance Security of Issuance Process (contd.)

Recommendation #1

- *Government / industry should dialogue about cross-application of existing security standards for identity issuance processes, and new standards development as appropriate*
- *Government / commercial ID issuers should give further attention to secure delivery of credentials to end user*

Issuance of Identity Credentials

Augment Private Sector Commercial Issuance Processes

Recommendation #2

- *Government / industry need to dialogue about greater interoperability between public / private sector ID theft prevention mechanisms*
  - Private sector could benefit from appropriate and secure access to government vital records systems

Issuance of Identity Credentials

Improve the Integrity of Identity Credentials

Recommendation #3

- *Document Security Alliance and North American Security Products Organization (NASPO) should proceed with project to measure effectiveness of document security technologies*
- *Department of Homeland Security should work with issue stakeholders to develop adversarial testing standards*
- *NASPO, SIA and SEMI in North America – and CEN in Europe – should proceed with standards for secure serialization anti-counterfeiting technology*

Exchange of Identity Data

Working Group 2 – Findings and Recommendations

Topics covered

- Strengthen Best Practices for Authentication
- Increase Understanding / Usability of Security Freezes

Exchange of Identity Data

Strengthen Best Practices for Authentication

Recommendation #4

- *Financial Institutions and credit grantors should take into account level of risk, cost and convenience when determining an appropriate authentication procedure*
  - Should not use easily-obtainable personal information such as Social Security numbers as sole authenticators
- *Financial regulatory agencies and FFIEC are encouraged to review the sufficiency of authentication practices for online banking*

Exchange of Identity Data

Strengthen Best Practices for Authentication (contd.)

Recommendation #4

- *Industry and standards developers are encouraged to continue to develop trusted networks for multi-factor mutual authentication*
- *Public and private sectors should implement systems to allow physical ID documents to be validated in real time*
- *FTC and financial regulatory agencies should provide guidance on best practices for credit grantors responding to fraud alerts*

Exchange of Identity Data

Strengthen Best Practices for Authentication (contd.)

Recommendation #4

- *Social Security Admin. should work with private sector on a mechanism that enables companies to verify if a Social Security number belongs to a minor*
- *Stakeholders should consider best practices / consumer education to help protect the elderly and terminally ill from fiduciary abuse*
- *Social Security Admin. should work with states and private sector to improve notification when someone is classified as deceased*
- *FTC should consider enhanced ID theft protection for active duty military*

Exchange of Identity Data

Increase Understanding / Usability of Security Freezes

Recommendation #5

- *Lenders, government agencies, consumer advocacy groups, credit reporting agencies and others should continue to support consumer education on benefits and limitations of security freezes*

Maintenance of Identity Information

Working Group 3 – Findings and Recommendations

Topics covered

- Enhance Data Security Management Best Practices
- Augment Best Practices for Sensitive Data Collection, Retention and Access
- Create Uniform Guidance on Data Breach Notification and Remediation

Maintenance of Identity Information

Enhance Data Security Management Best Practices

Recommendation #6

- *ISO/IEC, PCI Security Standards Council, NASPO and other standards developers should review / augment existing data security management standards (or develop new ones) to:*
  - Define the frequency of periodic employee security training and content of an employee awareness program
  - Clarify requirements for data access credentialing and background checks
  - Provide guidance on continuous review of access credentials and privileges

Maintenance of Identity Information

Enhance Data Security Management Best Practices (contd.)

Recommendation #6

- Develop targeted guidance for industry sectors that are not regulated or that do not have standards
- Provide guidance to ensure downstream vendors are secure
- Implement an ongoing program of security re-evaluation
- Develop a security breach risk assessment for insurance purposes

Maintenance of Identity Information

Augment Best Practices for Sensitive Data Collection, Retention and Access

Recommendation #7

- *Industry, Small Business Admin., Chambers of Commerce and similar organizations need to develop and distribute practical guidance for small businesses on data collection, retention and access*

- *Industry and key government stakeholders (FTC, OMB, SSA) need to develop uniform guidance on the collection, use and retention of Social Security numbers*

Maintenance of Identity Information

Create Uniform Guidance on Data Breach Notification and Remediation

Recommendation #8

- *Issue stakeholders need to dialogue on the desirability / feasibility of developing a private sector standard for data breach notification, recognizing there are tradeoffs*
- *Industry should assemble a cross-sector forum to develop uniform guidance on consumer remediation in the event of a data compromise*
- *Issue stakeholders should educate / reinforce ID theft prevention strategies to consumers*

ANSI IDSP - Phase 2 Charter (April 2008)

- Monitor / facilitate implementation of Panel's recommendations
- Continue to investigate new areas
- Provide a forum for information-sharing and cross-sector dialogue
- Maintain / enhance the standards inventory *[subject to funding becoming available]*

- Produce a progress report in one year

Current Activities – Identity Verification Standards

- Workshop launch meeting held July 7-8, 2008
- Explored the need for a national standard on identity proofing
  - Focused on issuance practices of government entities
  - Circularity caused by agencies relying on but not authenticating breeder documents issued by other agencies
- 24 participants from 17 organizations / agencies including
  - 5 federal government agencies (Nat'l Ctr for Health Statistics – part of the CDC, SSA, DHS, GSA and NIST)
  - 2 associations of state and local governmental officials in NAPHSIS (vital records offices) and AAMVA (motor vehicle administrators)
  - 2 ANSI-accredited standard developers in NASPO and ARMA.
- Agreement in principle to develop project plan for a national standard on identity proofing

Current Activities – Measuring / Reporting on ID theft

- Next workshop to be launched
- Will explore whether a standard for how research companies measure and report on identity theft would be a useful tool for industry, regulators and consumers
  - Some research companies publicize their methodology, while others do not
  - Controversies about research methodologies make it difficult to measure how well the marketplace is doing in combating ID theft and fraud

Current Activities – Plenary Meeting

- Review of current IDSP activities
- Updates on implementation of earlier panel recommendations
- Proposals for new workshops
- Information-sharing / networking
- To be held 4th Quarter 2008

International Activities – Privacy

- SCC (Canada) has requested the International Organization for Standardization (ISO) Technical Management Board (TMB) to revisit the issue of privacy
- Proposed topics to be explored included
  - Breach notification
  - Safety of kids online
  - Credential and Identity Management
  - Privacy Taxonomy and Information Model
  - Privacy impacts of new technology – such as RFIDs
  - Implementation of privacy laws and best practices
  - Protection of sensitive data – Health records, workplace info.

International Activities – Privacy (contd.)

- In June, ISO/TMB established task force (TF) on privacy
- To explore / advise on ISO technical standards that can support implementation of public policy initiatives on privacy, with specific focus on protection of personally identifiable information (PII) and fair information handling
- TF may inventory existing standards noting how they support public policy, but it shall not seek to drive public policy agendas
- IDSP will serve as virtual U.S. technical advisory group (TAG) to advise ANSI's expert to the TF

ANSI
American National Standards Institute

IDSP

To participate /
For more information

www.ansi.org/idsp

Jim McCabe
212-642-8921
jmccabe@ansi.org

BACK-UP SLIDES:
Background Information about the IDSP, ANSI and Standards Panels

IDSP Membership

- Membership in the IDSP is open to all affected parties. Representatives of industry, standards development organizations, trade and professional associations, government agencies, consumer groups, organized labor, academia and other groups are welcome. **Click here for a current list of IDSP member organizations.**
- **Sustaining Partners** join the panel with an annual fee of $25,000 in 2008. This entitles them to a seat on the panel Steering Committee, unlimited panel participants, full ANSI membership for 1 year, public recognition associated with this level of sponsorship, and recognition at the 2008 IDSP plenary meeting
- **Contributing members** join the panel with an annual fee of $6000 in 2008. This entitles them to a seat on the panel Steering Committee, two panel participants, basic ANSI membership for 1 year and public recognition associated with this level of sponsorship.
- **Panel participants** join with an annual per person fee of $1000 in 2008. Participants have access to panel materials and meetings.

ANSI Mission Statement

To enhance the global competitiveness of U.S. business and the American quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and ensuring their integrity.

ANSI American National Standards Institute

A Private- and Public-Sector Partnership Since 1918

American National Standards Institute (ANSI)

A Federation of members representing . . .

- Academia
- Individuals
- Government
- Manufacturing
- Trade Associations
- Professional Societies
- Service Organizations
- Standards Developers
- Consumer and Labor Interests
- and many more

ANSI is not a government agency or a standards developer.

Roles and Responsibilities of ANSI

- Accredit U.S. standards developing organizations and U.S. technical advisory groups
- Approves standards as American National Standards
- Provides access to international and regional standards bodies
  - U.S. member of International Organization for Standardization (ISO) and, via U.S. National Committee, International Electrotechnical Commission (IEC)
- Offers a neutral policy forum
- Accredits product, personnel and management system certification bodies, and testing and calibration laboratories
- Information provider
- Seller of publications

Standards Panel Roles

- Serve as a private/public sector forum for information sharing across sectors
- Identify and catalogue existing standards, guidelines and related conformity assessment systems
  - Recognize significant work already underway or that has been completed by a vast array of standards-setting bodies
- Facilitate the development and enhancement of standards to meet emerging national needs
  - Do not themselves develop standards
- Coordinate among many standards solutions being proposed

Standards Panel Deliverables

- Plenary meetings where information is gathered and work programs cultivated
- Workshops / working groups that evolve from the plenary discussions and further develop particular aspects of the issues
- Report / series of reports presenting the panel’s findings and recommendations which in turn drive future standards development activity

Other ANSI Sponsored Standards Panels

- **Healthcare Information Technology Standards Panel**
  Working with Dept. of Health and Human Services toward interoperable electronic health records
- **ANSI Nanotechnology Standards Panel**
  Responding to request from White House Office of Science and Technology Policy to take the lead in nanotechnology initiatives
- **ANSI Homeland Security Standards Panel**
  Providing Dept. of Homeland Security, 9/11 Commission, and federal agencies with the tools they need to address homeland security concerns
- **ANSI Biofuels Standards Coordination Panel**

  Promoting the development and compatibility of voluntary consensus standards and conformity assessment programs to support the large-scale commoditization of biofuels