Privacy and Other Policy Issues in Common ID for Federal Employees and Contractors

Ari Schwartz

Center For Democracy & Technology

Thank you!

CENTER FOR
DEMOCRACY
&
TECHNOLOGY

CDT's Mission

The Center for Democracy and Technology works to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies.

Learn more at: http://www.cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY

A Need for a Common ID Standard

- Government needs to be able to manage personnel and access
- HSPD-12 main goal: internal government management
- Broken ID systems:
  - are expensive
  - are not convenient
  - do not adequately protect security
  - do not adequately protect privacy

CENTER FOR DEMOCRACY & TECHNOLOGY

Process To Move Forward

- Doing IDs wrong would be worse than doing nothing at all
  - ID theft
  - Security leaks
- System must not create greater privacy and security risks
  - Progress is important
  - An integrated system is dependant on the weakest link
  - Don't let perfect system become enemy of a more secure and private system

CENTER FOR DEMOCRACY & TECHNOLOGY

Concerns With Current Implementation

- Technical standards are being set before policy framework
- Currently few policies to limit misuse and overuse of cards
- Specific technical concerns with FIPS201
- Training Issues

CENTER FOR DEMOCRACY & TECHNOLOGY

Concerns: Technical standards are being set before policy framework

- The business plan needs to come first!
- Agencies, employees and public are confused
  - Is this part of a bigger plan?
- Security and privacy require equal weight to:
  - People
  - Process
  - Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

Concerns: Currently no policies to limit misuse and overuse of cards

- Limits on private sector use of all backend data are needed
- Agencies need guidance on risk levels
- Overuse of the ID can be as bad as misuse
- Agencies should have to register uses

CENTER FOR DEMOCRACY & TECHNOLOGY

Concerns: Specific Technical Concerns

- Templates not images
  - Storage of actual fingerprint images on card is not worth risks
- Contactless chip
  - Added convenience currently may not be worth risks
  - Employees should be issued storage container for card when not in use
- Persistent ID
  - For federal government use only
  - Should not be on the front of the card
  - FIPS-201 offers a good technological solution: card ID and card holder ID are not on front of card
  - Policy for CHUID use is still important

CENTER FOR DEMOCRACY & TECHNOLOGY

Training

- Detailed privacy sensitivity and other policy training is needed for all levels
  - Issuers
  - All card holders
  - Security personnel

CENTER FOR DEMOCRACY & TECHNOLOGY

Applicable Policy

- Fair Information Practices --
  - http://www.cdt.org/privacy/guide/basic/fips.html
- Privacy Policy
  - Privacy Act of 1974
  - E-Government Act -- all agencies that are changing cards should do PIAs despite exemption
  - HIPAA rules for medical information
  - Privacy Oversight -- Chief Privacy Officers

CENTER FOR DEMOCRACY & TECHNOLOGY

Conclusions

- **Policy should have happened earlier in the process**
  - Privacy Impact Assessment is needed immediately
- **Guidance need not be micromanagement**
  - Risk levels for agencies
  - Limits private sector access
  - General policy guidance on training, security, redress rules for cards and card use
  - Technical mandates necessitate policy mandates!
- **No need take risks that may cost more in privacy, security, & fraud later**
  - Avoid mission creep at all costs

CENTER FOR DEMOCRACY & TECHNOLOGY

Contact

Ari Schwartz
Associate Director
CDT
http://www.cdt.org
202-637-9800
ari@cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY