Interagency Session
NSPD-59 and Identity Management

Duane Blackburn
Office of Science and Technology Policy
Executive Office of the President

September 22, 2009








Interagency Session
NSPD-59

Duane Blackburn
Office of Science and Technology Policy
Executive Office of the President

Brief History Recap

- 9/11
- NSTC Subcommittee on Biometrics and IdM
  - RDT&E Focus
  - Expand to standards and privacy
  - Address interoperability concerns
- NIP: Operational Issue
  - Partnership with NSTC
  - Strategic Framework for KSTs, approved by NSTC and NSC
- NSPD-59
  - KSTs
  - NSTs

Biometrics in Government Post 9/11: Advancing Science, Enhancing Operations

NSPD-59: Current Status

- Known and Suspected Terrorists (KSTs)
  - OMB and agencies integrating Strategic Framework into budget plans
  - Interim measures in place while full functionality is being developed
- National Security Threats (NSTs)
  - Reviewed some categories of individuals that don't quite rise to the level of terrorists to see how well the USG is identifying and screening for them.
  - KST-style approach not appropriate
  - Existing bi- (or multi-)agency approaches are working well
  - Continued assessments planned

NSPD-59: FAQs

- How can biometrics community help?
  - Standards; RDT&E
  - “Biometrics PD” is a misnomer
- How has the administration change impacted PD activities?
  - Key thrusts and personnel remain unchanged
  - Consolidation of HSC and NSC has been beneficial
- Can the PD be considered a success?
  - Pros: Raised stature of efforts with incoming appointees
  - Cons: Development of PD took lots of time and effort that we are still trying to recover from; addition of concurrent NST thrust sapped resources
  - Summation: Ask me in five years!








Interagency Session
Identity Management

Duane Blackburn
Office of Science and Technology Policy
Executive Office of the President

Government-supported Studies/Work

- President's Identity Theft Task Force
  - 2006-2007
- NSTC Task Force on Identity Management
  - Jan-Jul 2008
  - First Holistic Analysis
- NSTAC Identity Management Task Force
  - Dec 2008 – May 2009
  - External Advisory Committee
  - Initial tasking: Secure Authentication via Internet
- OECD/WPISP
  - Mar 2008 – June 2009
  - "The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers"
- CIO Council's ISIMC
  - Established 2008
  - Addressing USG Credentialing issues
- 60-day Cyber Security review
  - Feb-May 2009

Common Themes - Importance

- Identity Management is a critical, though often underappreciated, component of successful applications in a variety of sectors
- IdM can help remove barriers to collaboration and innovation by ensuring trust
- People/things have only one “true” identity, but several aliases with varying degrees of confidence in the linkages to the “true” identity.
  - How to enable and manage these identities properly in a single application is difficult, but is even more difficult across interconnected systems
- IdM activities in one application impacts and relies upon others, though these impacts aren’t normally understood or accounted for

Common Themes – R&D

- Technology available now is good, but improvements are needed to improve capabilities, resiliency, privacy protection, convenience and security
- Research is needed on how to best combine different technologies
- Researcher access to useful data is an inhibitor
- Side to side comparisons of technology options is difficult/confusing and isn't keeping pace with new products

Common Themes - Standards

- Interoperability is difficult if the systems do not share definitions and data structures
  - Increases the chance of errors, which would be propagated throughout the interconnected systems
- Market-based and consensus-supported standards most likely to be universally accepted
- The existence and use of universal standards (or lack thereof) is often viewed as an indicator of a market/technology's maturity

Common Themes - Privacy

- Improving IdM can actually enhance privacy protection over the status quo – if done properly
- Outreach is an important aspect of privacy policy
  - Even if the privacy policy is correct, negative public perception will scuttle a program quickly
- Privacy isn't just for lawyers
  - Building protections directly into the technology will provide greater assurance that the protections are implemented thoroughly and consistently.
- A single IdM privacy breach creates enduring problems in multiple systems
- Privacy and security aren't mutually exclusive

Common Themes – Need for Governance

- Identity-based systems are inherently connected to one another. Overall governance is required to manage this properly rather than ad-hoc or not at all
- All levels of government have the responsibility to ensure the safety and wellbeing of its citizenry – and IdM has clear impacts on national security, the economy, cyberspace, and individual healthcare
- Government must provide leadership and work with all stakeholders to create favorable conditions for the development of IdM that benefits users

Looking to the Future

- National dialogue
- Standards development
- Policy coordination
- Public/Private partnership

Duane Blackburn

dblackburn@ostp.eop.gov

202-456-6068