

# Interagency Advisory Board

*Meeting Agenda, August 25, 2009*

1. **Opening Remarks**
2. **Policy, process, regulations, technology, and infrastructure to employ HSPD-12 in USDA** (*Owen Unangst, USDA*)
3. **Policy and infrastructure for PIV use for Logical Access** (*Tim Baldrige, NASA*)
4. **NIST Update** (*Bill Macgregor, NIST*)
  - a) **Recent Publications**
  - b) **Safeguards built into PIV, and SP 800-116 recommendations**
5. **Leveraging Open Identity Standards for Gov't Interaction with American citizens** (*Chris Loudon*)
6. **Closing Remarks**

# **NIST PIV Status Update**

**William I. MacGregor**

**National Institute of Standards and Technology**

**IAB Meeting, 25Aug2009**

# Overview

- ***COMMENT PERIOD*** Draft SP 800-73-3
- ***DONE*** NISTIR 7611 “Use of ISO/IEC 24727”
- ***IN TEST*** PIV Card Trust Validation Refimp
- Biometric Match-On-Card Specification
- BIO Authentication Demonstration

# SP 800-73-3 Focused Update

*Comments due 13Sep2009, draft in*

*<http://csrc.nist.gov/publications/PubsDrafts.html>*

- Definition of UUID consistent with NFI spec
  - For Non-Federal cards used with PIV System
  - Not a proposal to change PIV Cards
- KMK: use with EC DH and RSA transport
  - Fully defined
- KMK: on-card retention of historical keys
  - Allow with certs on- or off-card
- Change Management Advice (Part 1, front)

# “Use of ISO/IEC 24727”

*NISTIR published*

- Based on lab demo of ISO/IEC 24727 middleware accessing a PIV Card
- Document describes the demo structure and purpose
- If possible, we will package and publish the demo source code
- Windows and Linux platforms, PC/SC below and CAPI or PKCS #11 above

# A REMINDER

When you hear “RFID cards can be cloned or skimmed”  
...are they talking about PIV?

Does the claim apply to the contact or contactless standard used  
by PIV? Or proximity or vicinity cards?

Please re-read SP 800-116, Section 4, and Appendix A,  
“Recommendations” Are they being followed?

Consider the use of multifactor authentication with independent  
factors. Can they all be cloned?

**Select the right Authentication Assurance Level!**

# Thanks for listening!

William I. MacGregor  
william.macgregor@nist.gov  
(301) 975-8721

<http://csrc.nist.gov>