# Special Pub 800-73 (Draft)

Jim Dray/Teresa Schwarzhoff

NIST Industry Day

November 18, 2004

# Design Goals

- Consider GSC-ISv2.1, PACS and PDMF

- Technology neutrality

- Standards compliance (ISO/IEC)

- Add card management

- Define an interoperable card platform for PIV credentials to support HSPD-12

# Nov. 8 Draft

- GSC-ISv2.1 Virtual Machine card edge
- Global Platform 2.0.1 compliant card manager
- ISO/IEC 7816-15 profile for key material

# FIPS 201 Phased Implementation

- Phase I
  - Agencies certify conformance to objectives of HSPD-12
  - NIST is publishing a GSC-ISv2.1 reference implementation
  - GSC-ISv2.1 + RI + PACS + PDMF
- Phase II
  - Migration to SP 800-73

# Comments on October 19 Draft

- 90%:  Not possible by October 2005
- 5%:  Should be object-oriented
- 5%:  Other
- Primary concern is clearly timeline
- Two-phased approach helps; actual dates to be established by OMB

# Summary

- SP 800-73 can be implemented on Virtual Machine cards by adding PIV applets

- SP 800-73 can be implemented on native cards by 'flashing' card OS or masking

- SP 800-73 is GSC-ISv3.0:  GSC-ISv2.1 plus card management

- Example migration report available at: http://csrc.nist.gov/piv-project