Mobile Biometrics Use case
Federal Protective Service

NIST Workshop
January 2013

Vince Eckert
Liaison to S&T
Department of Homeland Security
Federal Protection Service
The Federal Protective Service

- Director L. Eric Patterson
- 11 Regions
- Sworn Law Enforcement Officers – 900
- Protective Security Officers (Contracted) – 12,600
- Facilities – 9,000 (more than any other non-DoD agency)
Guard Accountability

• Current Challenge- Time and Attendance/ validation of training records
• Goal- Three Factor Authentication
• Industry Standards- FICAM, FIPS-201, NIST-116
• Cellular use case- Limited connectivity (WIFI, Ethernet or Internet) among the GSA portfolio
HOW????
Requirements

• Biometric- Integrated Biometric solution that has been certified to meet NIST SP800-76-2
• Card Technology- Integrated contact interface compliant with ISO/IEC7810 and ISO/IEC7816 and compatible with PIV, PIV-I
• Weather Proofing- MIL-STD-810G
• Display- text and color image data
• Communications- Cellular or direct internet connection
• Security- encrypted communications using a certified FIPS 140-2 encryption algorithm
• Data Pushed to Mobile device- Bolos....etc...
Questions?

Vince Eckert
Liaison to S&T
Department of Homeland Security
Federal Protection Service
vincent.e.eckert.ice.dhs.gov