Biometric Standards
ANSI Homeland Security Standards Panel
Ninth Annual Plenary Meeting
Will Graves, DHS/US-VISIT
November 9, 2010
Users of US-VISIT’s Biometric Identification and Analysis Services

Department of Justice

Department of State

Intelligence Community

Department of Defense

State and Local Law Enforcement

U.S. Secret Service

U.S. Customs and Border Protection

U.S. Coast Guard

U.S. Citizenship and Immigration Services

U.S. Immigration and Customs Enforcement

Transportation Security Administration

Federal Emergency Management Agency

UK Border Agency

Homeland Security
Standards

A document, established by consensus and approved by a recognized body, that provides rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

1Registry of USG Recommended Biometric Standards, Version 2.0, August 2009)
Why Biometric Standards?

• Ensure consistency in data definition
  • Meaning of the data
  • Usefulness of the data
• Enable data to be collected and used by different types of systems, and from multiple vendors
• Facilitate interoperability
• Reduce the cost of development and maintenance
• Enable testing of biometric system performance, as well as conformance to biometric standards
# Types of Biometric Standards

<table>
<thead>
<tr>
<th>Type of Standard</th>
<th>Why Needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Interchange</td>
<td>Necessary to achieve full data interchange and interoperability in a non-proprietary format</td>
</tr>
<tr>
<td>Technical Interface</td>
<td></td>
</tr>
<tr>
<td>Profiles</td>
<td>Define specific values, conditions, options described in relevant base standards to achieve specific requirements</td>
</tr>
<tr>
<td>Testing and Reporting</td>
<td>Specify and test the performance of identification and verification devices, algorithms, and systems</td>
</tr>
<tr>
<td>Conformance Testing</td>
<td>Verify vendor claims that their products conform to standards</td>
</tr>
<tr>
<td>Cross-jurisdictional and Societal Issues</td>
<td>Address study and standardization of technical solutions to societal aspects of biometric implementations excluding specifications for government applications.</td>
</tr>
</tbody>
</table>
Biometric Standards: Implementation

Technical Interface Standards
- BioAPI
  - INCITS/ISO/IEC 19784-1
  - INCITS/ISO/IEC 19784-2
  - INCITS 358
- CBEFF
  - INCITS 398
- BIAS
  - INCITS 442

Biometric Sample Capture

Transmission Profiles
- ANSI/NIST-ITL Base Standard
- IXM (DHS/US-VISIT)
- EBTS (DOJ/FBI)
- EBTS (DoD)
- INT-I (Interpol)

Biometric Recognition System
- Matching
- Storage

Data Format Standards for Collection, Storage, and Exchange

**Fingerprints, Plain and Rolled**
- Fingerprint -- Plain and Rolled Images
  - ANSI/NIST-ITL Type-4
  - ANSI/NIST-ITL Type-14
- Latent Fingerprint and Latent Palm Print Images
  - ANSI/NIST-ITL Type-13

**Palm Print Images**
- ANSI/NIST-ITL Type-15

**Fingerprint Minutiae and Latent Fingerprint Minutiae**
- ANSI/NIST-ITL Type-9

**Face Images**
- 2D Face Images
  - ICAO 9303 (ISO/IEC 19794-5)
  - ANSI/NIST-ITL, Type-10
- Iris Images
  - ANSI/NIST-ITL 2-2008, Type-17
Base Standard

A fundamental standard with elements that contain options. Different applications (e.g., criminal identification, traveler authentication) may require certain values for the optional elements. These options and conditions are defined in a ‘biometric profile’
Biometric Profiles

**Biometric [Application] Profile** – a conforming subset or combination of base standards used to effect specific biometric functions. Defines specific values or conditions from the range of options described in the base standards to support the interchange of data between applications and system interoperability.

**Biometric Transmission Profiles** define the sender and receiver specification for electronic communications between systems.
Transmission Profiles: Common Base
Transmission Profiles: Common Base
Locations of systems with the ANSI/NIST-ITL standard installed for data transfer (known to NIST)

Blue: National and International System Use
Red: State / Provincial / Local System Use

Source: NIST
IDENT Exchange Message - IXM

IXM is the IDENT XML biometric standard messaging format for interacting with US-VISIT IDENT Biometric Services

GJXDM/NIEM
- GJXDM (Global Justice) based
- Some NIEM elements
- Fully backward compatible

NIEM
- Add new services
- Fully NIEM conformant
Multi-modal biometrics interoperability

ISO/IEC 19794-5

ANSI/NIST Type-14

ISO/IEC 19794-6

ANSI/NIST Type-17

EBTS Msg

IXM Msg

IDENT

IAFIS/NGI

ABIS/DoD

ABIS/DoS

i:Identify

ANSI/NIST Type-10

ISO/IEC 19794-5

EBTS Msg

EBTS Msg

EBTS Msg

EBTS Msg
US-VISIT Biometric Standards

- Adoption and implementation of US-VISIT biometric standards
- IDENT requirements for transmission profiles; data interchange formats (fingerprint, palmprint, face and iris); data quality standards; NIST Mobile ID Best Practices
- Standards to achieve interoperability with
  - Federal stakeholders
  - Foreign countries (per agreements)
US Government Biometrics

Biometrics.gov Source of biometrics-related activities of the US Federal government to encourage collaboration and information sharing

Biometrics.gov/Standards Federal policies and guidance, Registry of USG Recommended Biometric Standards, posting of agency transmission specifications (e.g. for US-VISIT and DOD)

Biometrics Catalog Outreach to provide information to government and the public (http://www.biometricscatalog.org/)
William R. Graves
Chief of Biometric Standards and Technical Innovation Projects
Information Sharing & Technical Assistance Branch
william.graves@dhs.gov
202-298-5230
202-320-8469 (cell)