

An Overview of Biometrics

Peter T. Higgins

Higgins & Associates, International

202-625-7780

HigginsAssoc@aol.com

Session One

◆ State-of-the Art

- What are biometrics and how do they work
- Fingerprint recognition
- Face recognition
- Voice recognition
- Hand recognition
- Iris recognition

Session Two

- ◆ Implementation Issues & Challenges
 - Factors that influence the performance
 - What are some of the challenges
 - Applications for Homeland Defense and the INS
 - The role of biometric standards

Performance Factors

- ◆ Population Demographics
- ◆ Application
- ◆ User physiology
- ◆ User behavior
- ◆ User appearance
- ◆ Environment
- ◆ Sensor hardware
- ◆ User interface

Challenges

- ◆ Selecting appropriate biometric
- ◆ Developing operational concept with failure mode recovery
- ◆ Integrating it with current systems
- ◆ Educating and enrolling users
- ◆ Maintaining performance levels
- ◆ Testing system

Homeland Defense Issues

- ◆ Filter hype and science fiction
 - NASA report suggests use of brain & heart emissions for airport security
 - “Computers would apply statistical algorithms to correlate physiological patterns with computerized data on travel routines, criminal background and credit information from “hundreds to thousands of data sources.”
 - Washington Times 8-17-02

Homeland Defense Issues

- ◆ Number of traveler transactions
- ◆ Fall back position for timely resolution of alerts
 - *“That is my Trusted Traveler Card”*
- ◆ Limited availability of biometrically linked criminal histories
- ◆ Distributed data systems



Existing AFIS Databases

Other data checks

Current US AFIS Systems

◆ FBI

- Integrated Automated Fingerprint Identification System (IAFIS)
- National Crime Information Center (NCIC)
 - ◆ Fingerprint Matcher Subsystem

◆ INS

- IDENT two-finger AFIS system

Other Resources

◆ Name-based “*identification*” systems

■ NCIC

- ◆ Person and object records

■ NICS

- ◆ National Instant Check System - firearms licensing

■ National Law Enforcement Telecommunications System (NLETS)

FBI's IAFIS System

- ◆ 40+ million tenprint records in the repository
- ◆ 16 million searches per year, maxed at 81K per day
 - 48% criminal and 52% civil
 - 97% of criminal completed in under 2 hours; 24 hour turn around - civil
 - INS and OPM are largest contributors
- ◆ Afghan and Pakistani terrorist fingerprints added

FBI's NCIC System

- ◆ Primarily a name/number-based system:
 - Person and property information
- ◆ Fingerprint Matching Subsystem
 - Capacity for 250 K single finger records
 - Capacity for 3 to 5 K searches per day
 - ~300 fingerprint images in the repository
 - Three states participating

NCIC Details

- ◆ 3.3 million text transactions per day
- ◆ Complete accessibility to CCH files (III) Name or ID # based only
- ◆ Violent Gang and Terrorist File (VGTOF)
 - 2,000 name based terrorist suspects to-date
- ◆ 600,000 warrants posted (28% of total known)
- ◆ 314,000 persons ignoring deportation orders
- ◆ 652,000 Protective Orders (41 states)
- ◆ Convicted sex offender registry (39 states)

NCIC Details

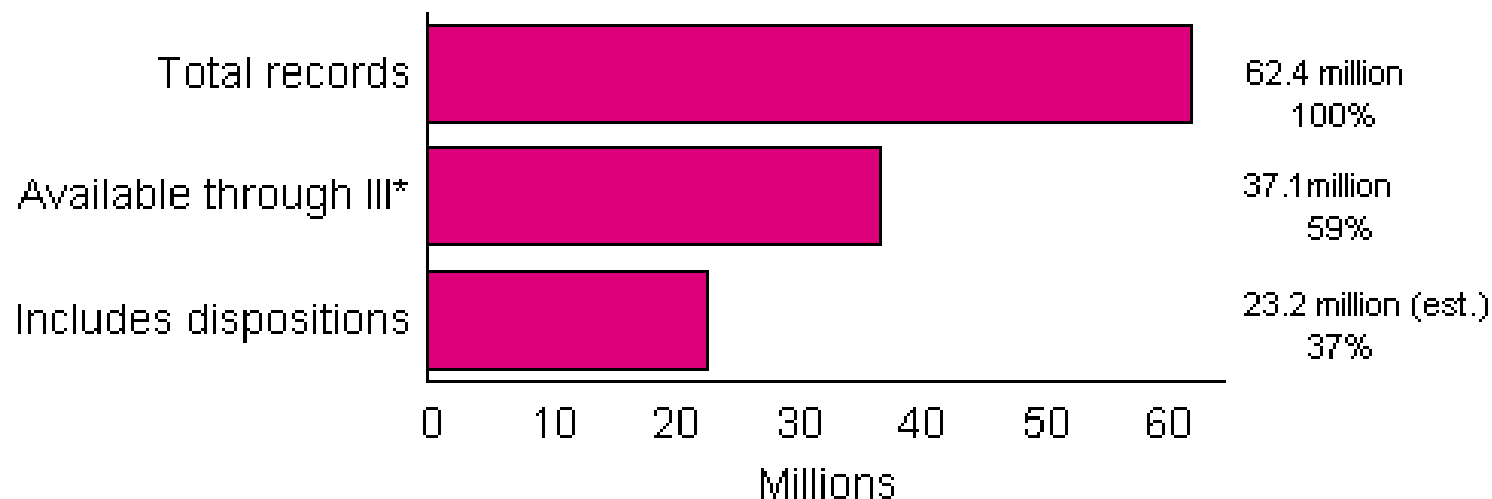
- ◆ Federal law now requires FBI to share certain files:
 - With INS for placement in their Lookout Database
 - With DOS for visas

NLETS Data Services

- ◆ 32 million transactions per month
- ◆ 13 million drivers license records; access to all DMVs
- ◆ Homeland security message key added
 - 45 states have programmed its use
 - OHS and FBI can send messages
 - ◆ Highest priority
 - ◆ Tailorable color codes

Availability & Completeness

Proportion of records in III and with dispositions, 1999



- Eighty-nine percent of the criminal history records maintained by the State criminal history repositories were automated. Approximately 6.2 million records, or 11%, were not automated.

2000 DOJ Report

FBI NICS Transactions

- ◆ 2.8 million *instant check* searches
January through May 2002
 - Not fingerprint-based
 - 1.3 M handled by FBI
 - ◆ 1.0 M (76%) immediate proceed
 - ◆ 19K denials (2%)
 - FBI - special data base
 - ◆ Illegal/unlawful aliens 2.5 K
 - ◆ Citizenship Renounced 12.6 K

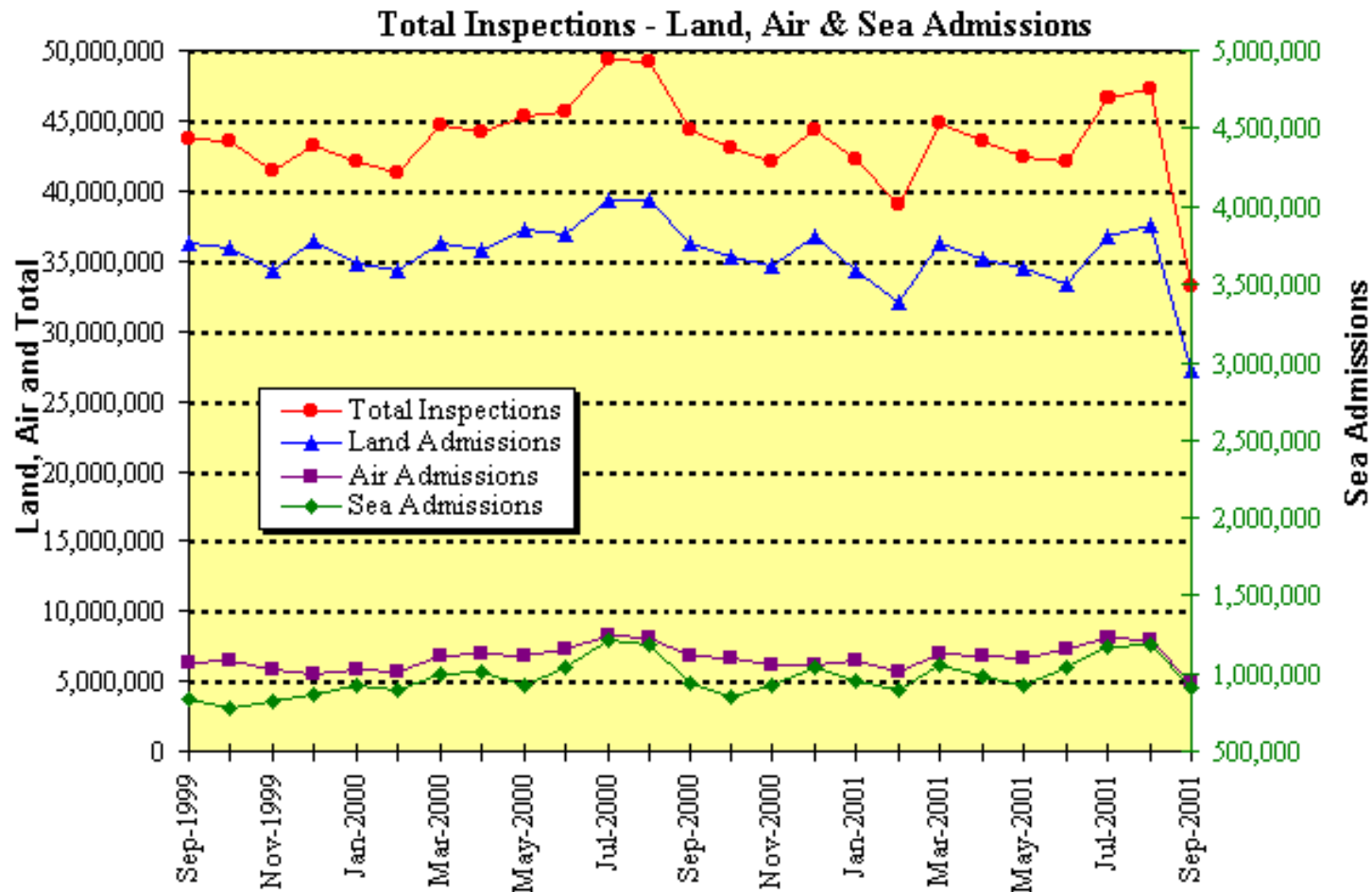
INS's IDENT System

- ◆ Border check system for illegal crossers
 - Two finger AFIS system with Mugshots
 - 2 minute turn around - 10,000 transactions per day
 - Repositories:
 - ◆ Recidivist 4,480 K
 - ◆ Lookout 378 K
 - ◆ Asylum 228 K

INS IDENT Services

- ◆ Border Patrol; Criminal Apprehension; and Benefit application process support
- ◆ Over 500 active LiveID workstations, geographically spread
- ◆ Short response time
 - Response includes photo and fingerprint as well as text record
 - Lower accuracy than full 10 print systems

Border Crossings



INS Challenge

- ◆ Check persons arriving & departing US
 - Search against IAFIS & IDENT repositories
 - About 36% are US citizens
 - Add each new border crosser so they can be tracked
- ◆ Annual transaction rates dwarf IAFIS
 - IAFIS 16 M CY 2001
 - Borders 540 M FY 2001 (in only)
 - Total **556 M**



How does all this relate to
Homeland Defense?



TSA Challenge

- ◆ Four distinct biometric application areas
 1. Employee identity verification and access authorization
 2. Protection of public areas in and around airports using surveillance
 3. **Passenger protection and identity verification**
 4. Aircrew identity verification

Passenger Id Verification

- ◆ Aircraft passengers checked for **TOWLs, etc.**
 - Daily
 - ◆ 1.6 million domestic & 0.2 million international boardings
 - Annually
 - ◆ ~650 million biometric checks - just for aircraft boarding
 - ~584 million are independent of INS

Passenger Id Verification

◆ Possible solution

■ Aviation Security Id Recognition Card

- ◆ Biometric enabled smart card

■ Proposed enrollment scheme

- ◆ Persons enroll at local airport or US Embassy

- 85 million people in the first year
- Often hundreds of miles away
- Similar proof as applying for Passport or Visa

Slides from Larry O’Gorman

Presented at
Stevens Institute of Technology
May 2002

Why Does it Reject Me?

- ◆ **Large throughput volume is the problem.**
- ◆ **Example:** <frequent flyer smart card with biometric>
 - Assume a system where each person is verified to their smartcard or a networked database by fingerprint.
 - If 5,000 people per hour are requesting access (Newark airport hourly passenger volume), in a 14 hour day, over *3,500 people will fail to be verified.*

How Many False Matches?

- ◆ **Example:** <face check vs. government database>
 - Assume a system that checks each face against a database of 25 suspected attackers with a best-case false match rate for face: 0.001
 - If 300 people are requesting Jumbo jet access, *7 of those will likely match suspected attackers.*
 - *How does 1 in 1000 rate result in 7 in 300 falsely matched?*

False Match Rate (FMR)

- ◆ **One problem is with more people in the database, there is more probability of false match.**
 - The effective FMR for facial id is a function of the number, n , of faces in the database.
 - False Match Rate for n : $FMR(n) = 1 - [1 - FMR(1)]^n$
- ◆ **Another problem is volume. The more matching attempts, the more false matches.**
 - $Total\ False\ Matches(N) = N \times FMR(n)$

False Matches

- ◆ **Example:** $FMR(1) = 0.001$, $n = 25$,
 $N = 300$ (example of previous page)
 - $FMR(n=25) = 1.0 - [1.0 - 0.001]^{25}$
 $= 0.025$ (2.5 in 100 vs. 1 in 1000)
 - $Total(300) = 300 \times 0.025 = 7$
suspected attackers to resolve

Federal Annual Challenge

- ◆ INS Inbound 540 million
- ◆ INS Outbound 540 million
- ◆ TSA Domestic 584 million
- ◆ Annual total 1.5 Billion
 - Or 100 times the current FBI capacity; noting that the processing is different.

Role of Standards

- ◆ What are Standards
- ◆ Who establishes them
- ◆ What biometric standards are available
- ◆ How stable are they?

IT Standards

The deliberate acceptance, by a group of people having common interests, of a quantifiable metric that influences their behavior and activities by permitting a common interchange.

- Official standards: ASCII
- De Facto Standards: Adobe pdf files

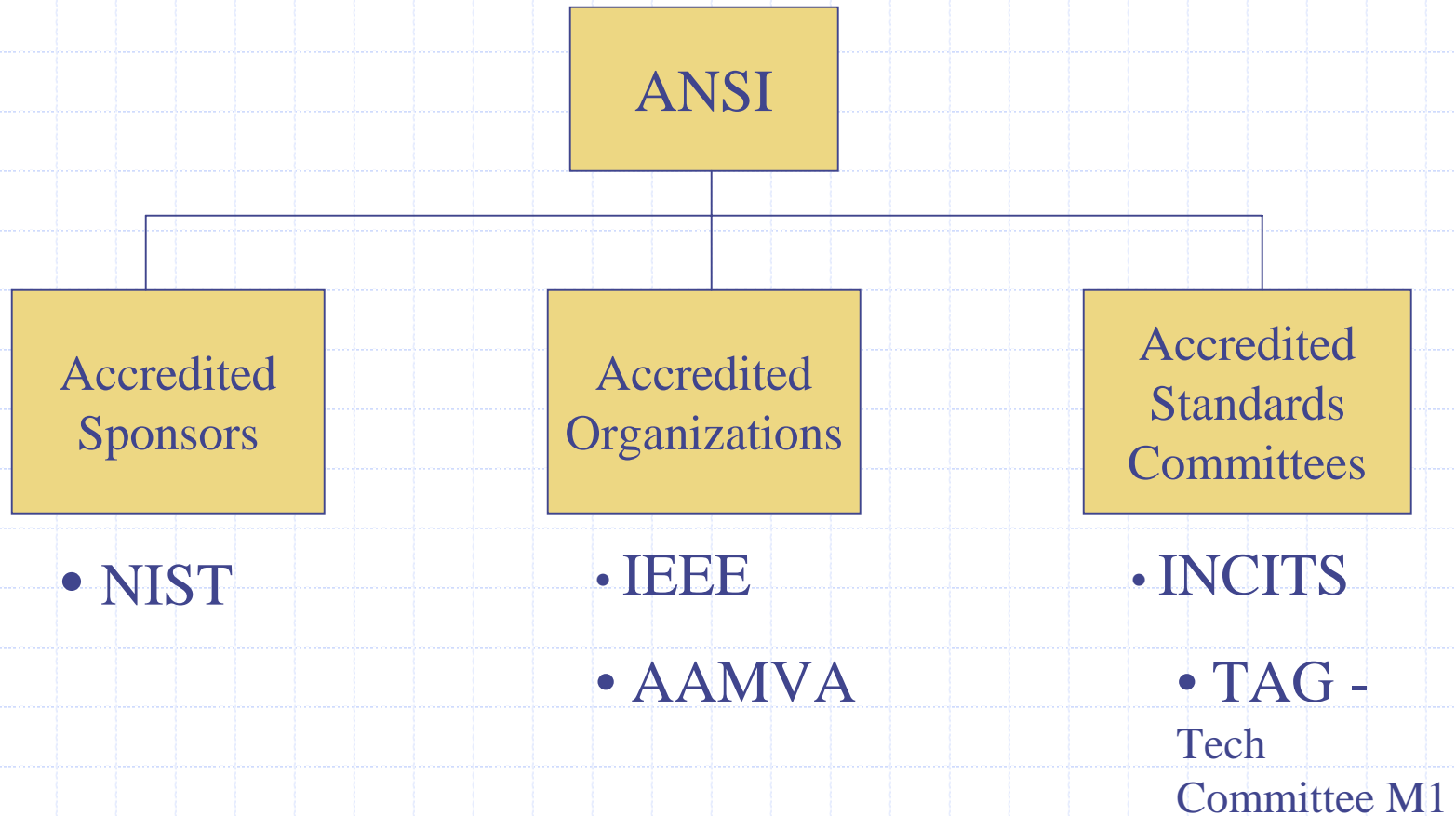
IT Standards

- ◆ ANSI approved US Standards organizations
 - **Accredited Sponsor** - e.g., NIST - workshops & canvases
 - **Accredited Organization** - e.g., IEEE, AAMVA
 - **Accredited Standards Committee** - e.g., Inter-National Committee for Information Technology Standards (INCITS)

Technical Committee M1

- ◆ Technical Committee M1, **Biometrics**
 - Established by the Executive Board of INCITS
 - Serves as the US Technical Advisory Group (TAG) for Biometrics providing recommendations to the INCITS & the JTC 1 TAG
 - Develops relationships with other INICTS Technical Committees and Subcommittees

American Standards



International Standards

- ◆ International Standards Groups
 - International Organization for Standards (ISO)
 - International Electrotechnical Commission (IEC)
 - International Telecommunication Union (ITU)

International Standards

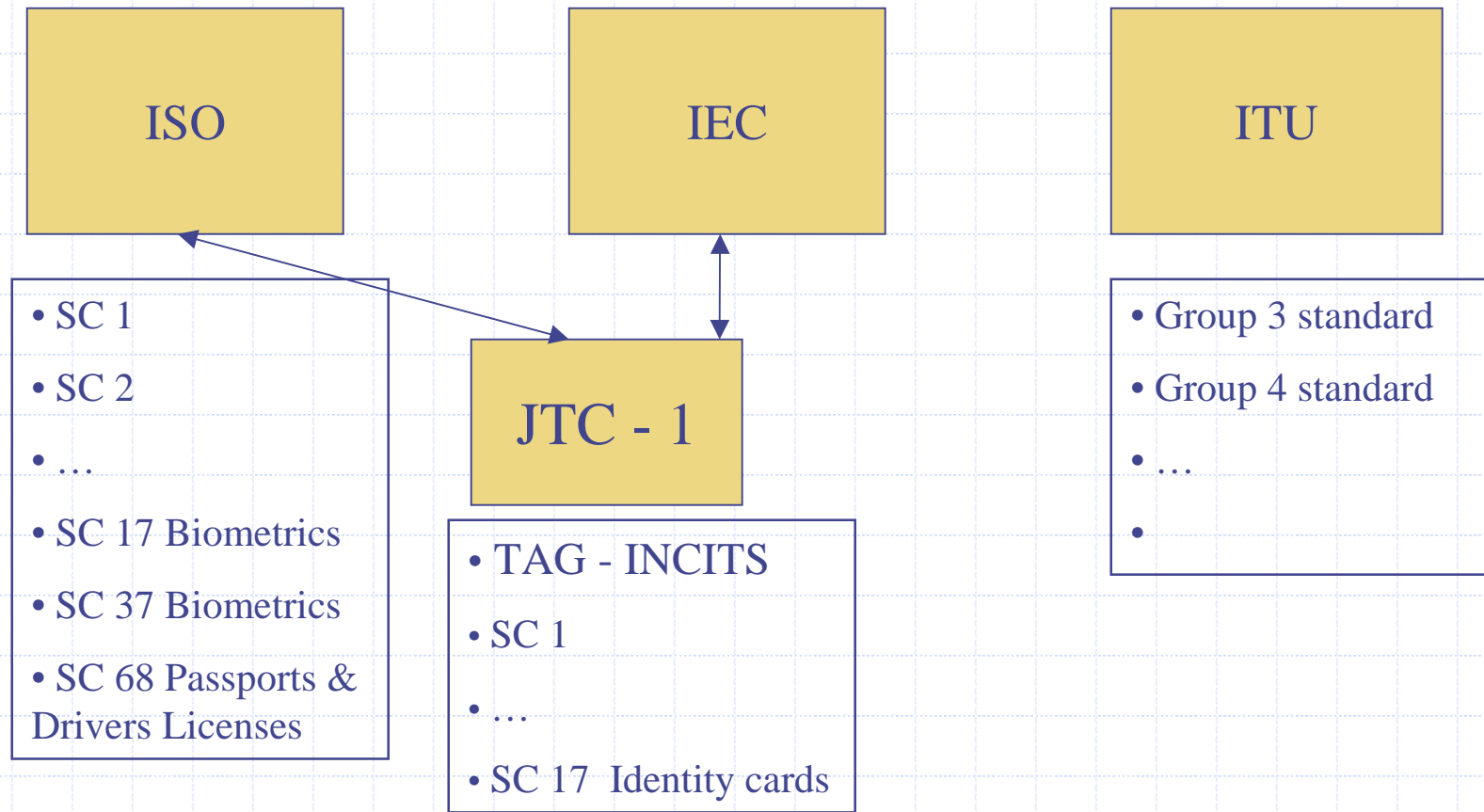
◆ ISO Subcommittees

- ISO 17 Biometrics
- ISO 68 Passports and Drivers Licenses

◆ Joint Committees

- ISO/IEC Joint Committee on Information Technology
 - ◆ aka Joint Technical Committee 1 (JTC 1)
 - ◆ JTC 1 has 19 subcommittees - at least one for biometrics

International Standards





Fingerprint Standards

Ten print

Standards Evolution

- ◆ 1993 Electronic Image Exchange - ANSI-NIST
- ◆ 1994 Image Quality followed - EFTS
- ◆ 1997 Facial images added
- ◆ 2000 Palm & variable density finger images

Why 1993?

- ◆ AFIS systems & livescans starting to proliferate
 - All using proprietary interfaces
 - Various image densities for scanners
 - Users had to resort to paper for data exchange

Why 1993?

- ◆ National response time - exceeded 6 months
 - Systems problem - required systems solution
 - ◆ Electronic capture
 - ◆ Electronic transmission
 - ◆ National repository for rapid searches
 - ◆ Electronic responses

ANSI NIST Standard (Continued)

◆ Key items in ANSI/NIST

■ Record types (1 - 16)

- ◆ Headers, fingerprint images, minutiae, mug shots, etc

■ Scan and transmission rates

■ Flexibility for different user communities of interest

- ◆ US, UK, Interpol, RCMP, etc.

ANSI NIST Standard (Continued)

- ◆ **Key items not in ANSI/NIST**
 - **Image quality**
 - ◆ the AFIS performance driver
 - **Data compression**
 - ◆ the communications and storage cost driver
 - **Single finger system standards**

Image Quality Standards

- ◆ Captured in EFTS Appendices F and G
 - A way to define minimum quality parameters for:
 - ◆ livescans, card scanners, and printers
 - Intended as:
 - ◆ FBI procurement guide
 - ◆ Threshold for submittal to the FBI
 - ◆ Now – widely used in procurements

Image Quality Standards

◆ Six criteria

- Geometric Image Accuracy
- Modulation Transfer Function
- Signal-to-Noise ratio
- Gray-scale Range of Image Data
- Gray-scale Linearity
- Output Gray Level Uniformity

Fingerprint Image Compression

- ◆ Wavelet Scalar Quantization (WSQ) compression
 - Current standard for 500 ppi images
 - Study for latent community drove FBI to 15:1 vice planned 20:1
- ◆ JPEG 2000 compression
 - Recommended approach for 1,000 ppi images
 - Initial look shows low level of data loss
 - Compression rate still in analysis, perhaps as low as 10:1

WSQ Description

- ◆ **Wavelet transform** - a completely invertible step in which no loss occurs. Applied to whole images not 8 X 8 pixel blocks as in JPEG.
- ◆ **Quantization stage** where a lossy scalar quantizer is used to assign similar wavelet coefficients to the same value.
- ◆ **Lossless compression** (Huffman encoding) where the quantized data are compressed to their final size.

Fingerprint Standards

Single Finger

NCIC 2000 Standard

- ◆ Single index finger
 - Right index finger
 - 500 ppi at 8 bits per pixel grayscale
 - Maximum image dimensions
 - ◆ Rolled images in repository: 1.6" X 1.5"
 - ◆ Flat search images: 0.88" x 1.2"
 - Converted by image processing with aspect ratio retained
 - ◆ 512 X 512 pixels
 - ◆ 1 bit per pixel - binary images

NCIC 2000 Standard

- ◆ Compressed at capture site
 - Average compression rate 127:1
- ◆ Features extracted at capture site
 - Printrak format
- ◆ Faces also captured and compressed

NCIC Update

- ◆ FBI evaluating migration to a set of more broadly adopted fingerprint standards
- ◆ Chicken & Egg problem
 - Not worth adding people until there are scanners everywhere
 - Not worth buying scanners until the repository is larger
 - ◆ Less than 300 fingers in system after 3+ years

AAMVA

- ◆ American Association of Motor Vehicle Administrators
 - States
 - Provinces
 - District of Columbia, Territories, etc.

AAMVA Standard

- ◆ Finger image capture
- ◆ Livescan - Flat print of at least two fingers
 - IQS per EFTS Appendix - G
 - 500 ppi at 8 bits per pixel grayscale

AAMVA Standard

- ◆ Image transmission
 - ANSI/NIST Type 1, 2, and 4 records
 - Compression following FBI WSQ spec.
- ◆ Minutiae storage and transmission
 - Fixed length header
 - Public and proprietary data
 - ◆ Close to Type 9 ANSI/EFTS Record
 - ◆ Plus vendor specific features or minutiae attributes

AAMVA Update

◆ Post 9-11

- New committees to look at standards
- New committees to look at use
- Congressional push for standard, biometrically enabled drivers licenses
 - ◆ Bill introduced June 2002



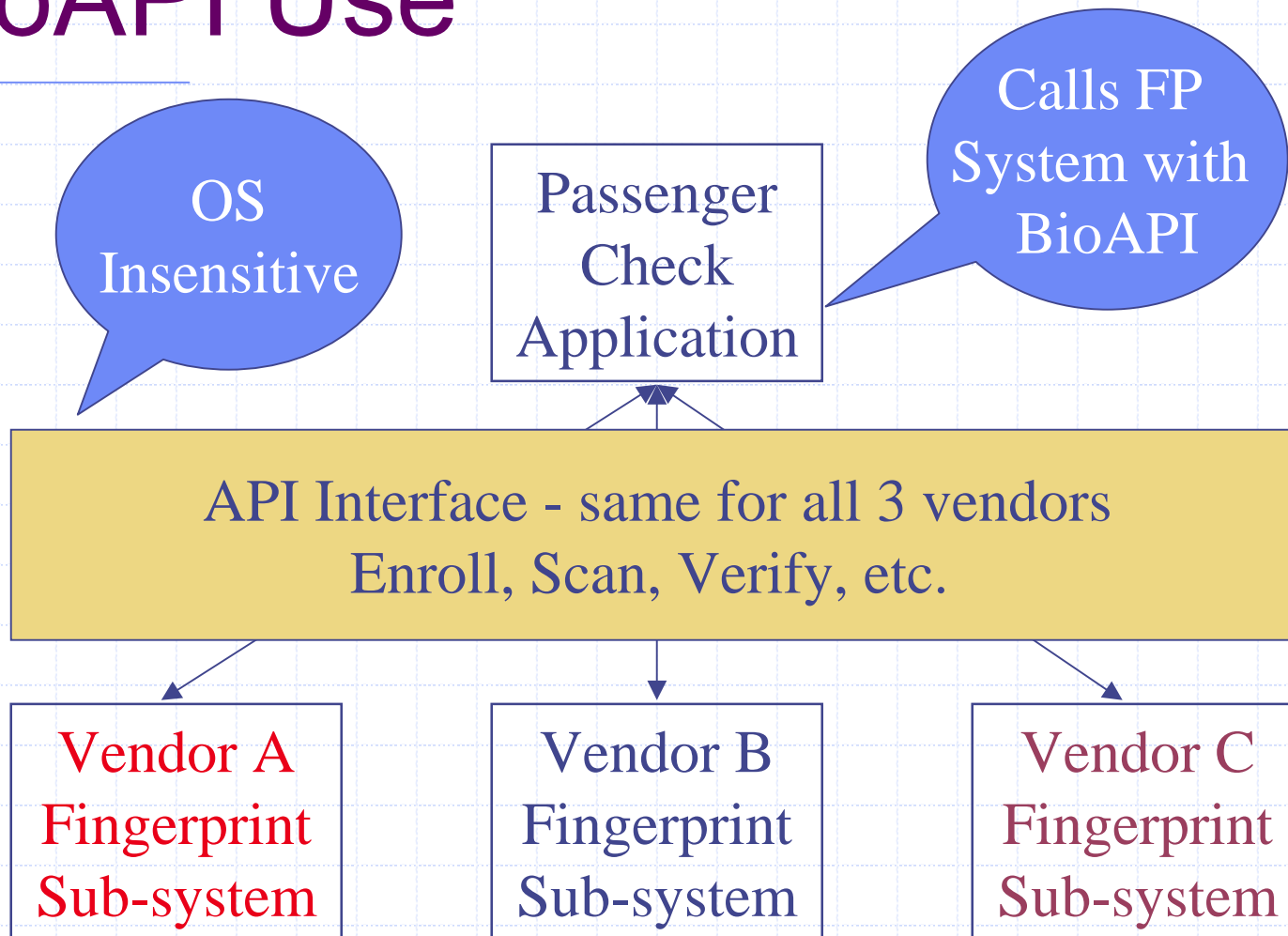
BioAPI Standard



BioAPI Standard

- ◆ Late 1990s parallel development of biometric APIs to permit applications to make standard calls independent of the biometric or vendor:
 - Novel SVAPI
 - BC HA-API
 - SafeLink Corp BioAPI
 - I/O Software BAPI
- ◆ Biometric Consortium took the lead to merge the efforts under BioAPI umbrella with strong NIST support

BioAPI Use



BioAPI Standard

◆ March 2002

- BioAPI Specification Version 1.1 was approved as ANSI/INCITS 358-2002
- INCITS M1 Technical committee resolved to support the transition of ANSI/INCITS 358-2002 to an ISO standard

Common Biometric Exchange File Format (CBEFF)

[NIST-ITL CBEFF Workshop B9]
NISTIR 6529-2001

CBEFF Standard

◆ Purpose:

*Define a common set of elements necessary to **support multiple biometric technologies** and to promote interoperability of biometric based application programs **and** systems by **allowing biometric database exchanges**.*

CBEFF Standard

- ◆ Requires an exchange agreement for an *Interoperability Domain*
 - Patrons - Standards Bodies (e.g., BioAPI)
 - Clients - Vendors and other standards bodies
 - Registration Authority - The IBIA

CBEFF Update

- ◆ An augmented version of CBEFF is under development by the NIST/BC Biometric Working Group

INCITS Press Release

- ◆ INCITS Technical Committee M1-Biometrics has approved project proposals for the development of five important biometric national standards (7/2002). The approved projects are:
 - 2 Biometric Application Profiles
 - 3 Biometric Data Format Projects

INCITS Press Release

- ◆ 2 Biometric Application Profiles:
 - Application Profile-Interoperability and Data Interchange-Biometrics Based Verification and Identification of Transportation Workers, and
 - Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Crossing

INCITS Press Release

- ◆ 3 Biometric Data Format Projects:
 - Finger Minutiae Format for Data Interchange,
 - Face Recognition Format for Data Interchange,
and
 - Finger Pattern-Based Interchange Format.

Patriot & Border Security Acts

- ◆ Mandates new standards to include biometric performance
- ◆ NIST assigned lead role

Patriot Act Border Security

- ◆ Identify background check for visa applicants
 - Enhance the FBI's IAFIS
 - Develop new AFIS for INS
- ◆ Verification check of visa presenter
 - Record one or more biometrics on memory chips
 - Use ANSI/NIST standard
 - Compare stored data to captured biometric

NIST Objectives

- ◆ To support PL 107-56
 - Determine the method to verify identity of persons applying for a visa
 - Determine the method to verify that the person having a visa is the same person that was issued the visa
 - Determine the estimates of performance of fingers and face
 - Develop and certify a technology standard based on one or more biometrics that have been determined to be highly accurate when used for identification & verification

NIST Objectives

- ◆ To support PL 107-173
 - Assisting the AG and Secretary of State to establish document authentication standards for tamper resistant entry and exit documents.

NIST Results To-date

- ◆ Fingerprints provide higher accuracy than face
 - Only have faces of most terrorists - multiple biometric might be required
- ◆ Fingerprint testing;
 - Thumbs give best results
 - Rolled to rolled comparisons give best results
 - Will develop a standard of performance

X9.84 Standard

- ◆ Developed by ASC X9 for financial industry
- ◆ Purpose:
 - Ensures the integrity and authenticity of biometric data*
- ◆ Status
 - Rejected for fast track
 - In normal approval process
 - De facto standard for financial industry

Stability of Standards

- ◆ Too many committees
- ◆ Too much politics
- ◆ Great concern by industry not to slight their biometric or its template
- ◆ Major effort required to follow processes and select standards to build to, to design systems around, or to specify as mandatory in procurements

Questions?



Contact Information

Peter T. Higgins

Higgins & Associates, International

Washington, DC

202-625-7780 (voice)

202-625-7781 (fax)

HigginsAssoc@aol.com (business)

PeterTHiggins@aol.com (personal)



End of Session 2