Files are in Adobe format.
Download the newest version from Adobe.

2011 Biometrics Conference

"National Security through Biometric Collaboration: A Roadmap to Tomorrow"

Arlington, VA

23 - 24 February 2011

Agenda

Wednesday , February 23, 2011

KEYNOTE SPEAKER
- Dr. Thomas Killion, *Director, Biometrics Identity Management Agency*

BIOMETRICS POLICY, PRIVACY, & SCREENING PANEL
- Dr. Lisa Nelson, *Assistant Professor, Graduate School of Public and International Affairs, University of Pittsburg*
- Melissa Ngo, *Esq., Privacy and Information Policy Consultant*

COLLECTION AND MATCHING PANEL
- Mr. Chris Miles, *Program Manager, U.S. Department of Homeland Security, Office of Science & Technology*
- Mr. Patrick Grother, *Director of Biometric Standards and Testing, National Institute of Standards and Technology (NIST), U.S. Department of Commerce*

COMMERCIAL PANEL
- Mr. Jon Dorsey, *Chief Executive Office, AllTrust Networks*
- Ms. Nicole Geller, *Program Manager, State Enterprise Solutions*

Thursday, February 24, 2011

KEYNOTE SPEAKER
- Mr. Charlie Wilson, *Partner, IDTechnology Partners*

FUTURES PANEL
- Ms. Maxine Most, *Principal, Acuity Market Intelligence*
- Mr. Peter O'Neill, *President, findBIOMETRICS*
- Dr. Stephanie Schuckers, *Associate Professor, Department of Electrical and Computer Engineering, Clarkson University*
- Mr. Luigi Tenore, *Chief Architect, U.S. VISIT, U.S. Department of Homeland Security*

INTERNATIONAL BIOMETRICS PANEL
- Ms. Gillian Ormiston, *Morpho UK Limited, formerly with European Commission, DG Justice, Freedom and Security*
- Mr. Padro Janices, *National Director ONTI, National Office of Information Technologies Undersecretariat of Management Technologies Secretariat of Public Management*

NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

2011 BIOMETRICS CONFERENCE

National Security through Biometric Collaboration: A Roadmap to Tomorrow

CONFERENCE HIGHLIGHTS INCLUDE:

Focused Panels:

- Biometrics Policy, Privacy, & Screening
- Collection and Matching
- Commercial use of Biometrics
- International Biometrics

"Biometrics in the Field" Address

FEBRUARY 23-24, 2011
WWW.NDIA.ORG/MEETINGS/1860

SHERATON NATIONAL HOTEL ▸ ARLINGTON, VA

EVENT #1860

2011 BIOMETRICS CONFERENCE

NATIONAL SECURITY THROUGH BIOMETRIC COLLABORATION: A ROADMAP TO TOMORROW

FEBRUARY 23-24, 2011 ▸ SHERATON NATIONAL HOTEL

The theme of the 2011 conference, "National Security Through Biometric Collaboration; A Roadmap for Tomorrow", recognizes the importance of engaging experts from multiple disciplines to address critical biometrics issues, challenges, and advancements especially relating to national defense in the years ahead. Strong collaboration among researchers, policy-makers and community stakeholders are essential for identifying and implementing promising, sustainable solutions that are relevant to the Warfighter and national interests. The 2011 conference will highlight successful partnerships that have evaluated or implemented policy or biometrics technologies and approaches for increasing the pace of scientific advancement.

DISPLAYS

The purchase of a display ($1,300) will include:

- Registration for one person (the person manning the display table)
- One standard 6 foot draped table and chair
- One electric hookup
- Overnight security

The displayer is welcome and encouraged to attend all events during the conference, including all scheduled continental breakfast, luncheons, reception, and sessions. Additional displayers must be registered for the conference as an attendee but may request a displayer ribbon on his/her badge.

All displays must be of the simple table-top/pop-up style standards. Space per pop-up display shall not exceed 6 ft. wide by 4 ft. deep. Minimal hardware to be utilized (computer systems for demonstrations are OK). No formal decorating company is involved. Companies must bring their own displays and plan to do their own set-up.

Displays will be sold on a first come, first serve basis and may sell out. Location of the display will be decided during move in and will also be on a first come, first serve basis.

To purchase a display, please visit www.ndia.org/meetings/1860.

SPECIAL NEEDS

NDIA Supports the Americans with Disabilities Act of 1990. Attendees with special needs should call Britt Bommelje at 703-247-2587 prior to February 11, 2011.

CONFERENCE ATTIRE

Appropriate dress for this symposium is business for civilians (coat and tie) and working uniform for military.

INQUIRES

For more information regarding the conference, please visit www.ndia.org/meetings/1860 or contact Britt Bommelje, at 703-247-2587 or bbommelje@ndia.org

LODGING

A block of rooms has been reserved at the Sheraton National Hotel. The government and industry rate is $207.00 U.S. (Single and Double).

In order to ensure the discounted rate, please make reservations early and ask for the NDIA room block. Rooms will not be held after January 24, 2011 and may sell out before then. Rates are subject to increase after this date.

Sheraton National Hotel
900 South Orme Street
Arlington, VA 22204

703-521-1900

SPONSORSHIP OPPORTUNITIES

$2,500 SPONSORSHIP INCLUDEDS

- Signage throughout the event
- Main podium recognition throughout the event

$5,000 SPONSORSHIP INCLUDEDS

- Signage throughout the event
- Company name on the back cover of the onsite brochure
- 350-word organization description in the onsite brochure
- Main podium recognition during the conference
- Hotlink on the conference website to your organization's website

$10,000 SPONSORSHIP INCLUDEDS

- Signage throughout the event
- Company name on the back cover of the onsite brochure
- 500-word organization description in the onsite brochure
- Main podium recognition during the conference
- Hotlink on the conference website to your organization's website
- Literature insert (one flyer, 8.5"X11", up to 4 pages, included in the information each attendee receives onsite, produced by the sponsoring organization)
- 3 complimentary conference registrations

**A Reception Sponsorship is also available. Please visit www.ndia.org/meetings/1860 and view the "Sponsorship" tab for details or to purchase a sponsorship.*

REGISTRATION INFORMATION:

Register online by visiting the conference website at www.ndia.org/meetings/1860. Online registration will close at 5:00 pm EST on February 11, 2011. You may also register by faxing the registration form found in this brochure to 703-552-1885 or mailing it to National Defense Industrial Association, Event # 1860, 2111 Wilson Blvd, Suite 400, Arlington, VA 22201. Payment must be made at the time of registration. Registrations will not be taken over the phone. In order for your name to appear in the on-site attendee roster, you must register for the conference by February 11, 2011. After this date, you must register onsite.

CONFERENCE REGISTRATION FEES	EARLY (BEFORE 1/12/11)	REGULAR (1/12/11 - 2/11/11)	LATE (AFTER 2/11/11)
GOVERNMENT/ ACADEMIA/ ALLIED GOV.	$425	$470	$520
INDUSTRY NDIA MEMBER	$525	$580	$640
INDUSTRY NON-NDIA MEMBER	$600	$660	$725

CANCELLATION POLICY:

Cancellations received before February 11, 2011 will receive a refund minus a $75 cancellation fee. No refunds will be given for cancellations received after February 11, 2011. Substitutions are welcome in lieu of cancellations. Cancellations and substitutions must be made in writing to Britt Bommelje at bbommelje@ndia.org.

THE REGISTRATION FEE INCLUDES:

- 2 continental breakfasts listed in the agenda
- 4 networking breaks listed in the agenda
- 2 networking luncheons listed in the agenda
- Networking reception on February 23, 2011
- Attendance to general session
- Admission to the displays

BIOMETRICS POLICY, PRIVACY, & SCREENING PANEL

This structured forum will explore both the informational as well as personal privacy implications of biometrics. From the public sector to the private sector, large-scale deployments are being perceived by some as privacy invasive and by others as privacy protective -- this panel will explore both sides of the issue.

COLLECTION AND MATCHING PANEL

Leaders from a broad range biometrics programs, applications and research will present on various areas of biometrics collection, its challenges, best practices, successes stories and future visions from their perspective.

COMMERCIAL PANEL

This panel will provide examples of successful application of identity management systems used by industry today and systems planned and desired for future adaptation.

WEDNESDAY, FEBRUARY 23

6:00 am - 11:45 am Set-up Displays

7:00 am - 6:30 pm Registration Open

7:30 am - 8:30 am Continental Networking Breakfast

8:30 am - 5:00 pm **GENERAL SESSION**

8:30 am **WELCOME AND OPENING REMARKS**

- MG Barry Bates, USA (Ret), *Vice President, NDIA*
- Mr. Jim Carlson, *Chair, Industrial Committee on Biometrics*
- Mr. Jerry Jackson, *Conference Chair, Biometric Service Account Manager, IBM - Global Business Services*

9:00 am **KEYNOTE SPEAKER**

- Dr. Thomas Killion, *Director, Biometrics Identity Management Agency*

9:45 am **BIOMETRICS POLICY, PRIVACY, & SCREENING PANEL**

Moderator: Mr. Samir Nanavati, *Partner, International Biometrics Group*

Panelists:

- Mr. Jim Harper, *Director of Information Policy Studies, The CATO Institute*
- Mr. Chris Calabrese, *Project Counsel, American Civil Liberties Union, Technology & Liberty Project*
- Dr. Lisa Nelson, *Assistant Professor, Graduate School of Public and International Affairs, University of Pittsburg*

11:45 am - 1:00 pm Networking Luncheon

WEDNESDAY CONTINUED

1:00 pm **COLLECTION AND MATCHING PANEL**

Moderator: Dr. Charles Li, *Technical Director, Border Security, Identity Management and Biometrics, Raytheon Intelligence & Information System*

Panelists:

- Mr. Chris Miles, *Program Manager, U.S. Department of Homeland Security, Office of Science & Technology*
- Mr. Steve Yonkers, *Deputy Assistant Director for Business Policy and Planning, U.S. Department of Homeland Security, U.S. VISIT*
- Mr. Nick Megna, *Supervisory Management and Program Analyst, FBI CJIS Division, Next Generation Identification Program, FBI*
- Ms. Angela Miller, *Chief, Emerging Technologies Branch, Office of Consular Systems and Technology, U.S. Department of State*
- Mr. Patrick Grother, *Director of Biometric Standards and Testing, National Institute of Standards and Technology (NIST), U.S. Department of Commerce*

3:25 pm - 3:45 pm Networking Break

3:45 pm **COMMERCIAL PANEL**

Moderator: Mr. Ramon Reyes, *Business Development Manager, MorphoTrak*

Panelists:

- Mr. Jon Dorsey, *Chief Executive Office, AllTrust Networks*
- Ms. Nicole Geller, *Program Manager, State Enterprise Solutions*

5:00 pm - 6:30 pm Networking Reception

CONFERENCE PLANNING COMMITTEE

- Chair: Mr. Jerry Jackson, *IBM - Global Business Services*
- Ms. Joyce Augustyn, *Biometrics Identity Management Agency*
- Mr. Jim Carlson
- Mr. Steve Charles, *Raytheon Company*
- Mr. John Christensen, *Northrop Grumman Corporation*
- Mr. Magruder Dent, *Aware, Inc.*
- Ms. Penny Eastman, *L-1 Identity Solutions, Inc.*
- Dr. Stephen Elliott, *Purdue University*
- Mr. Glenn Hickok, *Cross Match Technologies, Inc.*
- Dr. Charles Li, *Raytheon Intelligence & Information System*
- Mr. Samir Nanavati, *International Biometric Group*
- Mr. Dan Nickell, *Croftware, LLC*
- Mr. Ramon Reyes, *MorphoTrak*
- Ms. Cheryl Waldrup, *Daon, Inc.*
- Mr. Mike Via, *Senior Systems Engineer, National Interest Security Company, LLC*

THURSDAY, FEBRUARY 24

7:00 am - 3:45 pm Registration Open

7:00 am - 8:15 am Continental Networking Breakfast

8:15 am - 3:45 pm **GENERAL SESSION**

8:15 am **OPENING REMARKS**

8:30 am **KEYNOTE SPEAKER**

- Mr. Charlie Wilson, *Partner, IDTechnology Partners*

9:15 am - 9:45 am Networking Break

9:45 am **FUTURES PANEL**

Moderator: Mr. Dan Nickell, *Principal, Croftware, LLC*

Panelists:

- Ms. Maxine Most, *Principal, Acuity Market Intelligence*
- Mr. Peter O'Neill, *President, findBIOMETRICS*
- Dr. Stephanie Schuckers, *Associate Professor, Department of Electrical and Computer Engineering, Clarkson University*
- Mr. Luigi Tenore, *Chief Architect, U.S. VISIT, U.S. Department of Homeland Security*

11:30 am - 1:00 pm Networking Luncheon

1:00 pm **INTERNATIONAL BIOMETRICS PANEL**

Moderator: Mr. John Christensen, *Account Executive, Northrop Grumman Corporation*

Panelists:

- Ms. Gillian Ormiston, *Morpho UK Limited, formerly with European Commission, DG Justice, Freedom and Security*
- Mr. Padro Janices, *National Director ONTI, National Office of Information Technologies Undersecretariat of Management Technologies Secretariat of Public Management*

2:00 pm - 2:30 pm Networking Break

2:30 pm **BIOMETRICS IN THE FIELD**

- Lt Col Tom Pratt, USMC, *Military Operations Branch Chief, Biometrics Identity Management Agency*

3:30 pm **CLOSING REMARKS**

- Mr. Jerry Jackson, *Conference Chair, Biometric Service Account Manager, IBM - Global Business Services*

3:45 pm **CONFERENCE CONCLUDES**

FUTURES PANEL

The Futures Panel will be made up of experts from a broad range of disciplines and perspectives. The panelists will address various aspects of biometrics "futures" in which they have expertise. "Future" describes developments to be realized within the next 5-10 years.

INTERNATIONAL PANEL

The International Panel will be made up of leaders and experts from a broad range of biometrics programs, applications and research; consequently, each panelist will discuss ongoing & future identity management programs within their country, opportunities for collaboration, and best practices.

EVENT #1860 ▸ NDIA REGISTRATION FORM

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION ▸ 2111 WILSON BOULEVARD, SUITE 400 ▸ ARLINGTON, VA 22201-3061
(703) 522-1820 ▸ (703) 522-1885 FAX ▸ WWW.NDIA.ORG

2011 BIOMETRICS CONFERENCE ▸ SHERATON NATIONAL HOTEL ARLINGTON, VA ▸ FEBRUARY 23-24, 2010

3 WAYS TO SIGN UP:

1. **Online with a credit card at www.ndia.org**
2. **By fax with a credit card - Fax: (703) 522-1885**
3. **By mail with a check or credit card**

▷ Address Change Needed

NDIA Master ID/Membership # _____ Social Security # _____
(If known - hint: on mailing label above your name) *(Last 4 digits - optional)*

Prefix *(e.g. RADM, COL, Mr., Ms., Dr., etc.)* _____

Name: First _____ MI ____ Last _____

Military Affiliation _____ Nickname _____
(e.g. USMC, USA (Ret.) etc.) *(For meeting badges)*

Title _____

Organization _____

Street Address _____

Address *(Suite, PO Box, Mail Stop, Building, etc.)* _____

City _____ State _____ Zip _____ Country _____

Phone _____ Ext. _____ Fax _____

E-Mail _____

Signature* _____ Date _____

PREFERRED WAY TO RECEIVE INFORMATION

Conference Information	▷ Address above	▷ Alternate (Print address below)	▷ E-mail
Subscriptions	▷ Address above	▷ Alternate (Print address below)	

Alternate Street Address _____

Alternate Address *(Suite, PO Box, Mail Stop, Building, etc.)* _____

City _____ State _____ Zip _____ Country _____

* By your signature above, you consent to receive communications sent by or on behalf of NDIA, its Chapters, Divisions and affiliates (NTSA, AFEI, PSA, WID) through regular mail, e-mail, telephone or fax. NDIA, its Chapters, Divisions and affiliates do not sell data to vendors or other companies.

CONFERENCE REGISTRATION FEES

	Early *(Before 1/12)*	Regular *(1/12-2/11)*	Late *(After 2/11)*
Government/Academia[1]	$425	$470	$520
Industry NDIA Member and affiliates (AFEI, NTSA, PSA, WID)	$525	$580	$640
Industry non-NDIA member[2]	$600	$660	$725
Display Registration	$1300	$1300	$1300

All cancellation, substitution, and refund requests must be submitted in writing no later than February 11, 2011 to NDIA, attn: Britt Bommelje via e-mail at bbommelje@ndia.org. There is a $75 cancellation fee for all refunds. Refunds will not be given for no-shows. If an attendee shows a balance and does not attend the conference, he/she will be invoiced for payment. This cancellation policy applies to all attendees regardless of their method of registration or reason(s) for cancellation.

Substitutions are welcome in lieu of cancellations. All substitutions must be made in writing to Britt Bommelje at BBommelje@ndia.org.

[1] *Includes a free three-year NDIA membership and subscription to* National Defense *magazine for military and government employees.*

▷ No, do not sign me up for the free government membership.

[2] *Registration fees for non-NDIA (or affiliate) members include a one-year non-refundable NDIA membership —$15.00 will be applied for your 12 month subscription to* National Defense *magazine.*

PAYMENT OPTIONS

▷ **Check** (Payable to NDIA - Event #1860) ▷ **Government PO/Training Form #** _____

▷ **VISA** ▷ **MasterCard** ▷ **American Express** ▷ **Diners Club** ▷ **Cash**

If paying by credit card, you may return by fax to 703-522-1885.

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Credit Card Number ☐☐/☐☐ Exp. Date

Signature _____ Date _____

BY COMPLETING THE FOLLOWING, YOU HELP US UNDERSTAND WHO IS ATTENDING OUR EVENTS.

PRIMARY OCCUPATIONAL CLASSIFICATION. Check ONE.

- ▷ Defense Business/Industry
- ▷ R&D/Laboratories
- ▷ Army
- ▷ Navy
- ▷ Air Force
- ▷ Marine Corps
- ▷ Coast Guard
- ▷ DOD/MOD Civilian
- ▷ Government Civilian (Non-DOD/MOD)
- ▷ Trade/Professional Assn.
- ▷ Educator/Academia
- ▷ Professional Services
- ▷ Non-Defense Business
- ▷ Other _____

CURRENT JOB/TITLE/POSITION. Check ONE.

- ▷ Senior Executive
- ▷ Executive
- ▷ Manager
- ▷ Engineer/Scientist
- ▷ Professor/Instructor/Librarian
- ▷ Ambassador/Attaché
- ▷ Legislator/Legislative Aide
- ▷ General/Admiral
- ▷ Colonel/Navy Captain
- ▷ Lieutenant Colonel/Commander/ Major/Lieutenant Commander
- ▷ Captain/Lieutenant/Ensign
- ▷ Enlisted Military
- ▷ Other _____

Year of birth _____
(optional)

QUESTIONS, CONTACT:

BRITT BOMMELJE

PHONE: 703-247-2587

E-MAIL: BBOMMELJE@NDIA.ORG

MAIL REGISTRATION TO:
NDIA - EVENT #1860
2111 WILSON BOULEVARD
SUITE 400
ARLINGTON, VA 22201

FAX TO: 703-522-1885

DHS Science & Technology:

Biometrics Collection and Matching

Mr. Christopher Miles, Biometrics Program Manager
Human Factors/Behavioral Sciences Division

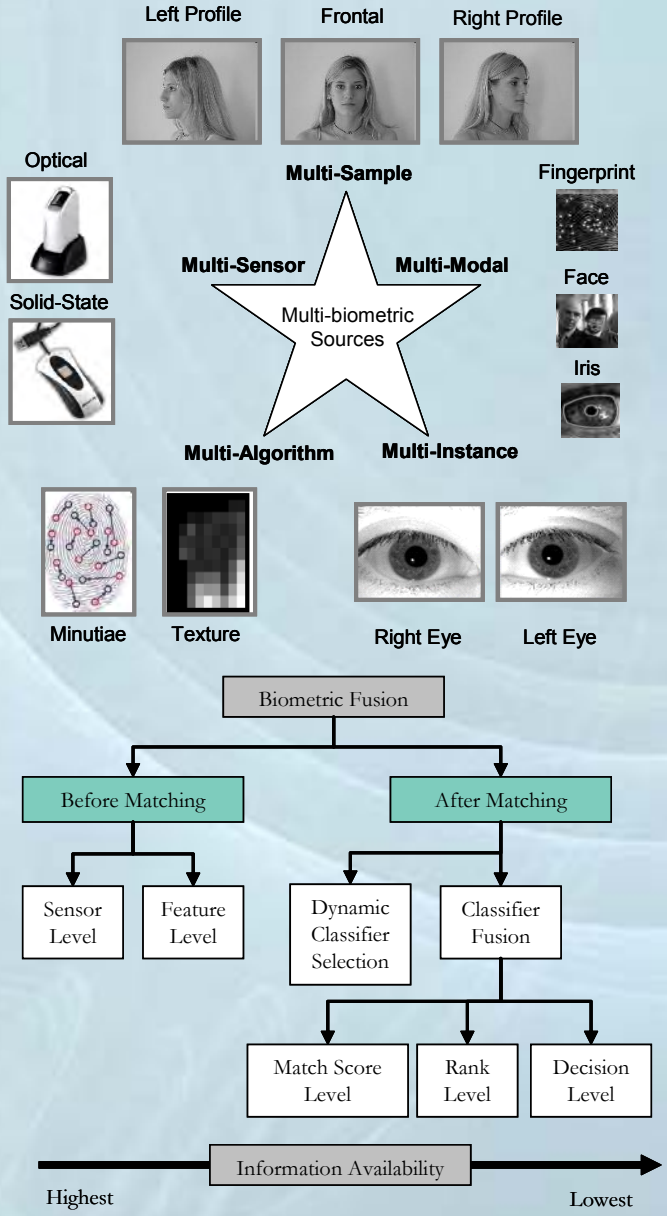
Science and Technology Directorate
Department of Homeland Security

February 23, 2011

Homeland Security

Multibiometrics – Plenty of Challenges

Characteristic	Definition
1. Universality	Every individual accessing the application should possess the trait.
2. Uniqueness	The given trait should be sufficiently different across individuals comprising the population.
3. Permanence	The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.
4. Measurability	It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired data should be amenable to processing in order to extract representative feature sets.
5. Performance	The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
6. Acceptability	Individuals in the target population that will use the application should be willing to present their biometric trait to the system.
7. Circumvention	This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g. fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.



Homeland Security

A. Ross, K. Nandakumar, and A.K. Jain. *Introduction to Multibiometrics* and *Handbook of Multibiometrics*.

Multibiometrics – Plenty of Challenges

Robust and Novel Acquisition: Innovative methods of acquiring biometric information and novel or emerging biometric modalities.

Fusion Approaches:

- **Dynamic Decisional Fusion**
- **Hierarchical Fusion**
- **Quality Enhanced Fusion Schemes**
- **Fusion Incorporating Meta/Ancillary Data**
- **Hybrid Fusion**
- **Sensor-Level Fusion**
- **Rank-Level Fusion**
- **Multi-Sensor Fusion**

Homeland Security

Multibiometrics – Plenty of Challenges

Observing the Biometric Menagerie: Careful examination of match score distributions as well as the observance and analysis of problematic subjects.

Biometric Capacity Analysis: Analysis of the theoretical system capacity of the template representation and the biometric variations observed during inter and intra-class comparisons.

Model Estimation/Update Schemes: Modeling update schemes to trigger the re-evaluation of system thresholds, re-estimation of relevant densities, or selection of different algorithms for classification.

Homeland Security

Multibiometrics – Plenty of Challenges

Multi-Biometric Indexing Systems: Investigating the ability to index based on multiple biometric sources to minimize the penetration rate (percentage of the database searched) without adding additional errors due to incorrect indexing.

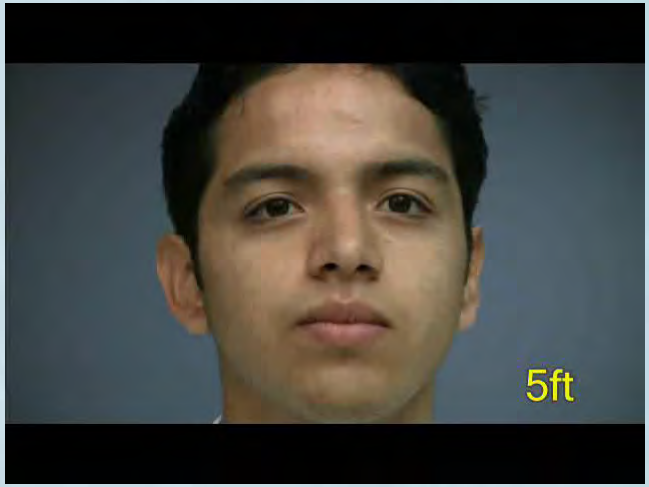
Addressing Multi-Biometric Vulnerabilities: Analysis of circumvention approaches for multibiometric identification, verification, and watchlist systems.

Homeland Security

Multibiometric Resource – Free Data

Q-FIRE: Quality – Face & Iris Research Ensemble

- 200 person data collection varying quality factors of illumination, resolution, angle, focus and motion
- Used in NIST Iris Quality Calibration and Evaluation (IQCE) to test influence of quality metrics' on iris recognition accuracy
- Available to researchers:
  Dr. Stephanie Schuckers, ECE
  sschucke@clarkson.edu



Sample Q-FIRE Face Images

Sample Q-FIRE Iris Images

Homeland Security

Mobile Screening or Enrollment?

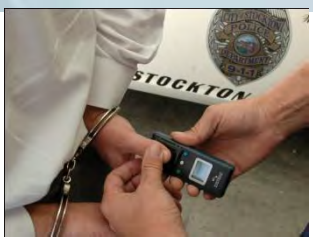
Goal: Obtain operational information on use and performance of state of the art mobile biometric and multi-modal biometric devices from law enforcement end-users

Objectives:

- Pilot next generation mobile biometric devices and obtain operational feedback from federal/state/local/tribal partners
- Demonstrate potential for discovering terrorist nexus through use of mobile devices in field, e.g. access to DHS/FBI databases
- Feedback to DHS S&T HFD for next BAA development

Current Device Performance

- Two print and thumb (rolled) – *10 print with larger devices*
- Facial and Iris recognition/enrollment
- Latent print imaging
- Date, time and GPS stamp
- LAN connectivity
- On-board "watch lists" with capability up to 100,000 records

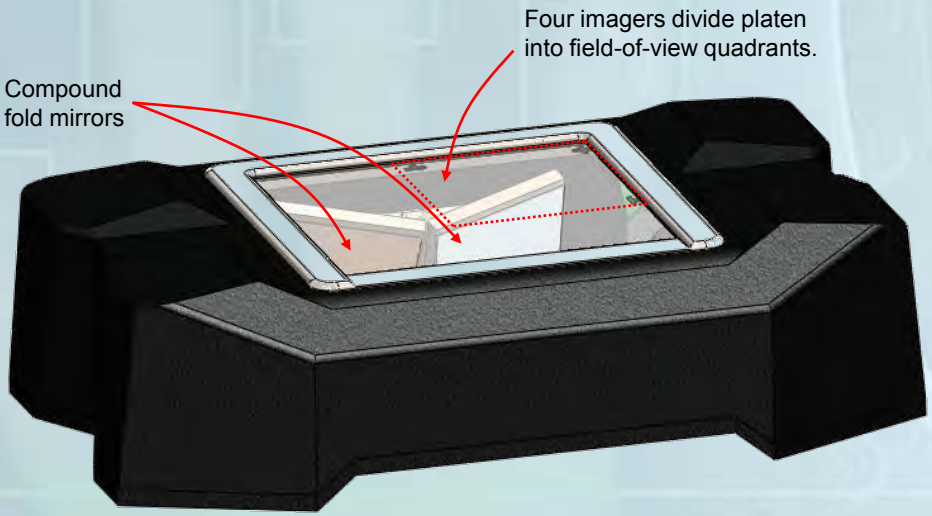


Participants and Deployments

- DHS/ICE Western Region
- DHS/ICE – Alamosa, CO
- WA State Criminal Justice Training Commission
- LAPD
- Pima County, AZ Sheriff
- Stockton, CA PD
- Marietta, GA PD
- St. Croix, WI Tribal Police
- Pinellas County, FL Sheriff
- Gwinnett County, GA Sheriff
- DeKalb Marshal, GA

Four Finger Slap Module

Southwest Research Institute

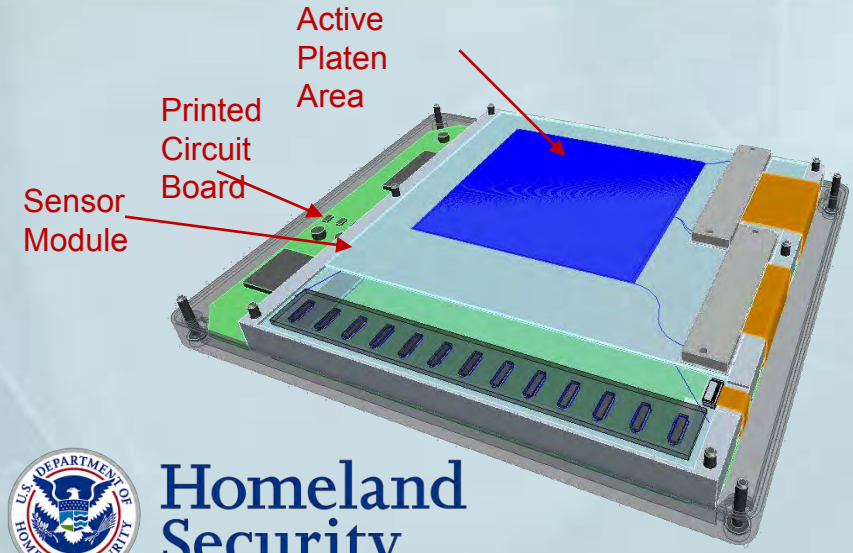


Specification	SwRI Proposed System
Resolution	500 ppi
Dimensions	7.9” x 5.1” x 2.1”
Weight	< 1.5 lbs
Capture area	3.2” x 3.0”
Usage	In/Outdoor, highly portable
Print Types	Single prints 4-Slap prints Rolled prints
Processing time	<5 sec per slap,<3 sec per flat, <8 sec per rolled
Architecture	Stand-alone or peripheral

Homeland Security

Four Finger Slap Module

L-1 Identity Solutions



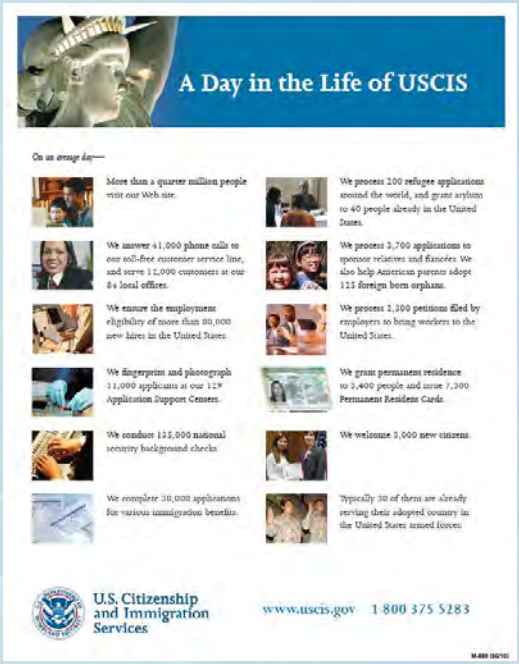
Specification	L-1 Proposed System
Resolution	500 ppi
Dimensions	6” x 7.5” x 1”
Weight	< 2 lbs
Capture area	3.2” x 3.0”
Usage	In/Outdoor, highly portable
Print Types	Single prints 4-Slap prints
Processing time	10 sec for 4-4-2
Architecture	Stand-alone or peripheral

Homeland Security

DNA: Creating a New Biometric

Needs and Requirements Findings:

- On an <u>average DAY</u> in the life of USCIS:
  - 400 refugee applications processed worldwide
  - 40 persons in the US are granted asylum
  - 3700 applications to sponsor relatives and fiancées entry to the United States
  - 100 foreign born orphans are adopted by American parents
  - Fingerprints and photographs are taken of 11,000 applicants at the 133 Application Support Centers (ASC)
  - 135,000 national security background checks are conducted
  - 3,400 persons are granted citizenship (30 are serving in the US military)

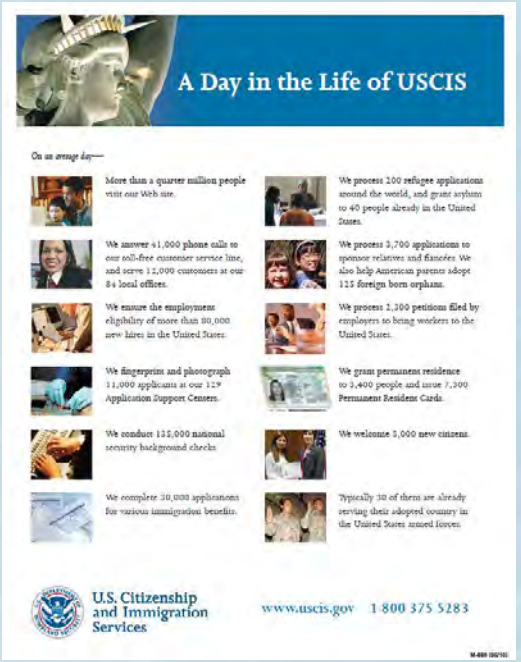


Homeland Security

DNA: Creating a New Biometric

Needs and Requirements Findings:

- DHS Needs to Verify Family Relationships
  - Kinship for Asylum and Refugee cases
  - Kinship for Adoptions
  - Kinship for Child Smuggling/Border Trafficking
- DHS to Identify Known Criminals
  - Immigration
    - DNA Criminal Check is not redundant to fingerprint check
  - CBP Border Violators & ICE Detainees
    - DOJ mandate to collect DNA from all detained persons
- DHS also Needs DNA for Mass Casualty and Missing Persons Identification



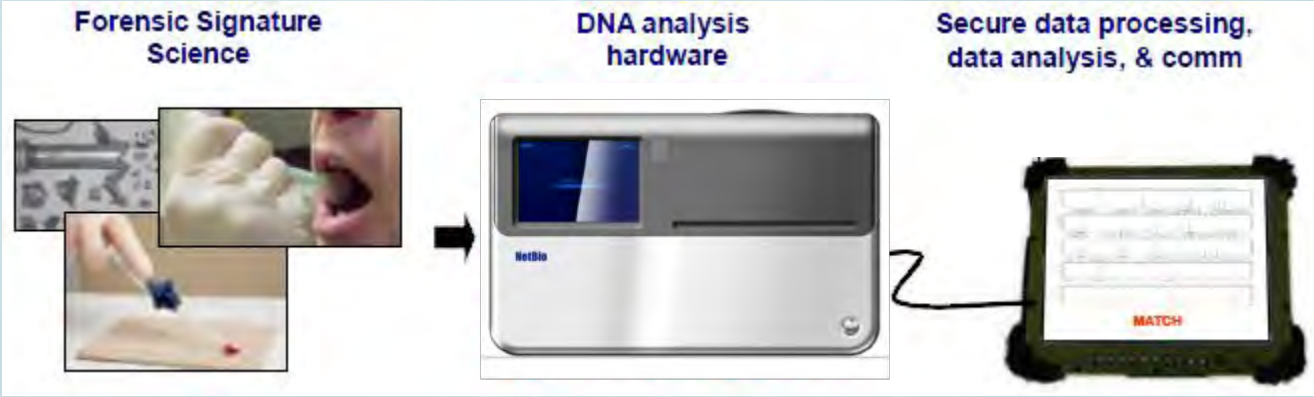
Homeland Security

DHS S&T Rapid-DNA Screening

"Accelerated Nuclear DNA Equipment"

Jointly funded DoD, DOJ, DHS Project

- Conduct 18 month R&D effort to develop prototype system
- Initial desktop-size, automated system with low-volume unit cost of $275K available 6 months after prototype
- Current manual processing steps automated and integrated into a desktop-size device
- Delivery of Prototype in 18 months

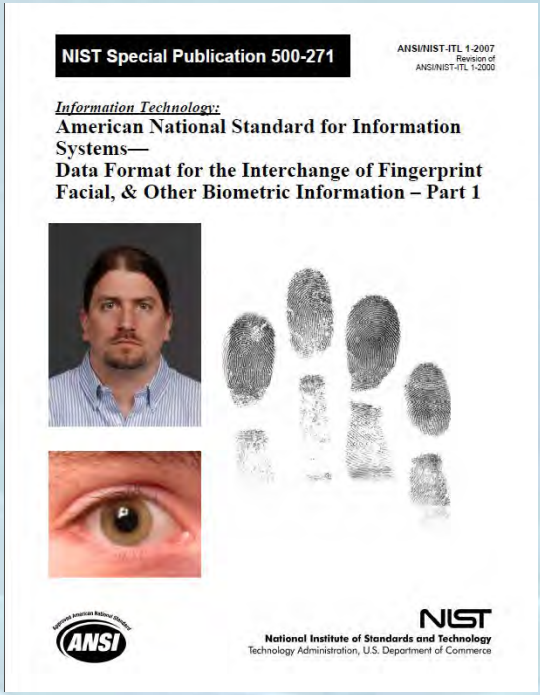


Homeland Security

Rapid-DNA Data Sharing Standards

ANSI/NIST-Information Technology Laboratory (ITL)

- First published in 1986
  - exchange of fingerprint information
- Updated in 2007 and 2008
  - Iris exchange
  - Conformance to other standards - XML
  - Updated facial and fingerprint specifications
- 2011 update underway
  - Adds a DNA and Kinship record in addition to other significant changes
  - Meeting next week (March 1-3) at NIST



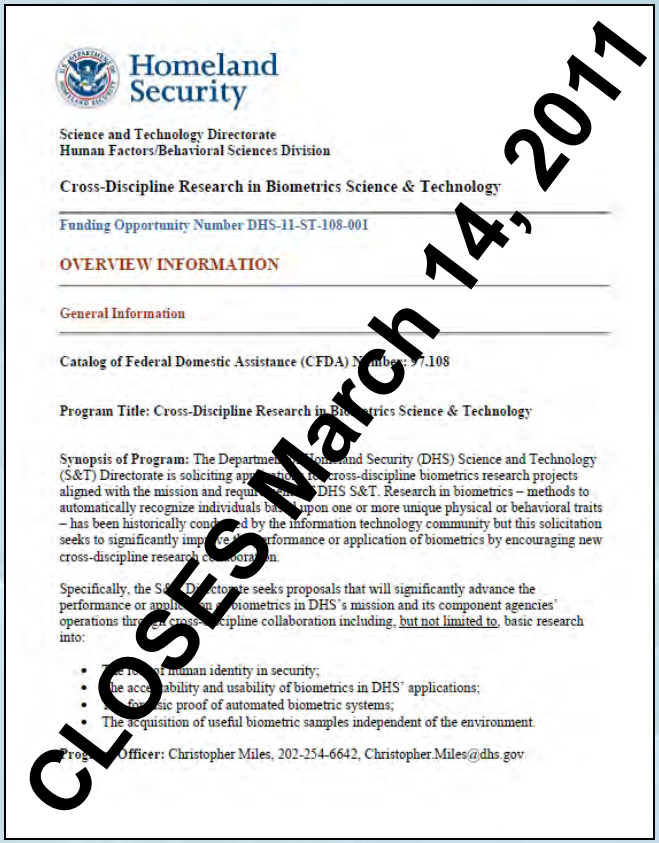
http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

Homeland Security

Cross-Discipline Challenges

Cross-Discipline Research in Biometrics Science & Technology

- Funding Opportunity Number: DHS-11-ST-108-001 at www.Grants.gov
- Encourages cross-discipline biometrics research projects aligned with DHS mission and requirements
- Substantial participation must be shown by two or more scientific disciplines.
- Domestic & foreign accredited institutions of higher education (domestic must take the lead)


Homeland Security

Science and Technology Directorate
Human Factors/Behavioral Sciences Division

Cross-Discipline Research in Biometrics Science & Technology

Funding Opportunity Number DHS-11-ST-108-001

OVERVIEW INFORMATION

General Information

Catalog of Federal Domestic Assistance (CFDA) Number 97.108

Program Title: Cross-Discipline Research in Biometrics Science & Technology

Synopsis of Program: The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate is soliciting applications for cross-discipline biometrics research projects aligned with the mission and requirements of DHS S&T. Research in biometrics – methods to automatically recognize individuals based upon one or more unique physical or behavioral traits – has been historically conducted by the information technology community but this solicitation seeks to significantly improve the performance or application of biometrics by encouraging new cross-discipline research collaboration.

Specifically, the S&T Directorate seeks proposals that will significantly advance the performance or application of biometrics in DHS's mission and its component agencies' operations through cross-discipline collaboration including, but not limited to, basic research into:

- The role of human identity in security;
- The accessibility and usability of biometrics in DHS' applications;
- Forensic proof of automated biometric systems;
- The acquisition of useful biometric samples independent of the environment.

Program Officer: Christopher Miles, 202-254-6642, Christopher.Miles@dhs.gov

CLOSES March 14, 2011

Homeland Security

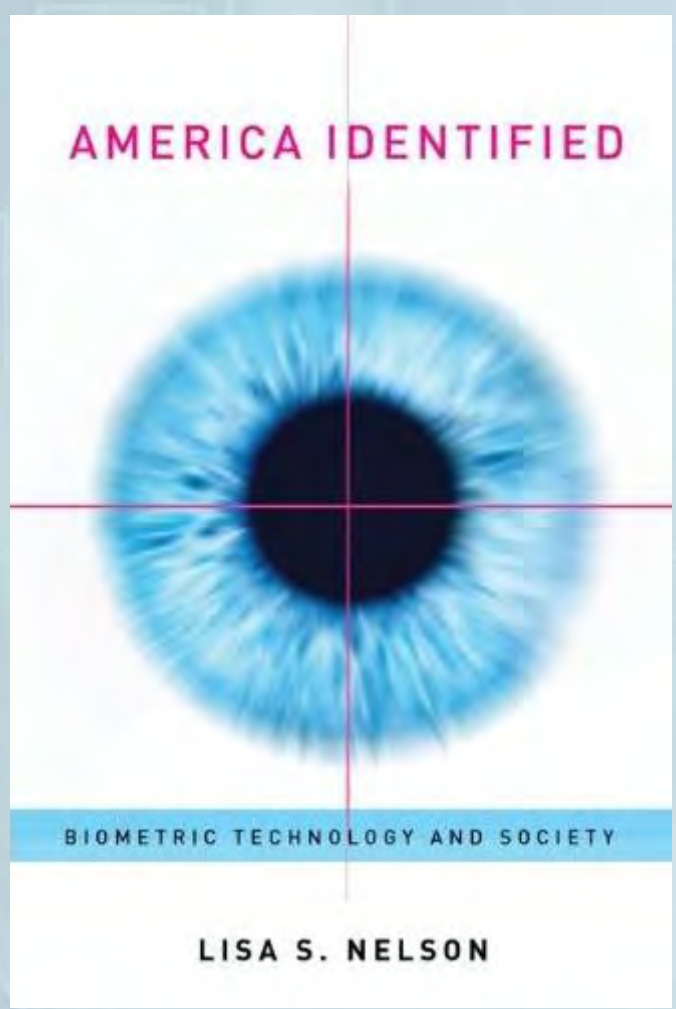
Cross-Discipline Challenges

Cross-Discipline Research in Biometrics Science & Technology

- The role of human identity in security
  – combining biometrics and cryptography
- Acceptability and usability of biometrics in DHS' apps.
  – combining biometrics with mathematics, cognitive psychology, industrial design and/or behavioral sciences
- Forensic proof of automated biometric systems
  – combining biometrics and forensic or medical sciences
- Acquisition of useful biometric samples independent of the environment
  – combining biometrics with complimentary imaging disciplines
- Other cross-discipline topics that significantly enhance biometrics science and technology

Homeland Security

Acceptability and Usability



America Identified: Biometric Technology and Society

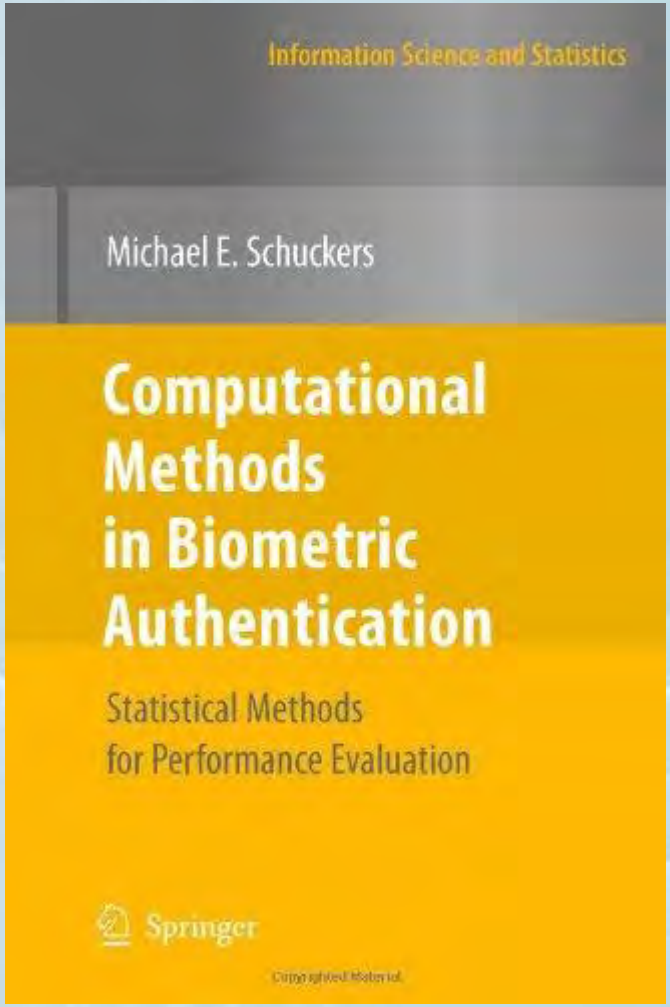
- Provides an overview of the societal perception of identification technologies and biometrics
- Addresses privacy, anonymity, trust, paternalism and the impact of 09/11
- Results of surveys and discussion panels support a clear federal role for biometric security solutions
- Published by MIT Press in December 2010

Homeland Security

Acceptability and Usability

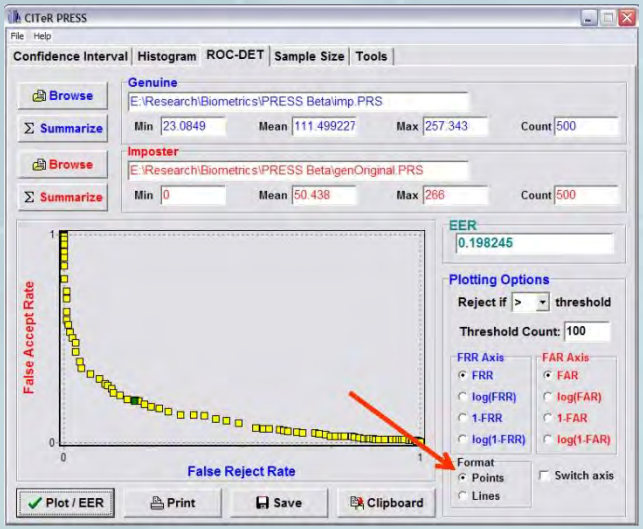
Computation Methods in Biometric Authentication

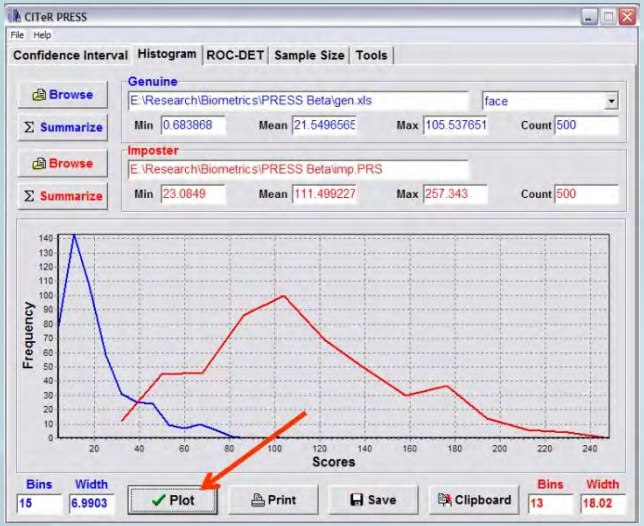
- Statistical methods for biometric performance metrics including: false non-match rate, false match rate, failure to enroll, failure to acquire and the receiver operating characteristic curve
- Allows for the comparison of two or more of these metrics
- More than 120 examples
- Published by Springer, 2010



Homeland Security

Acceptability and Usability





PRESS v.2: Program for Rate Estimation and Statistical Summaries

- Software Tool to implement the methods in Computational Methods in Biometric Authentication
- Confidence intervals, genuine vs. imposter histograms, EER calculations and ROC curves
- Tool for determining sample sizes needed for data collections
- Available as Freeware at: http://myslu.stlawu.edu/~msch/biometrics/book/software.html

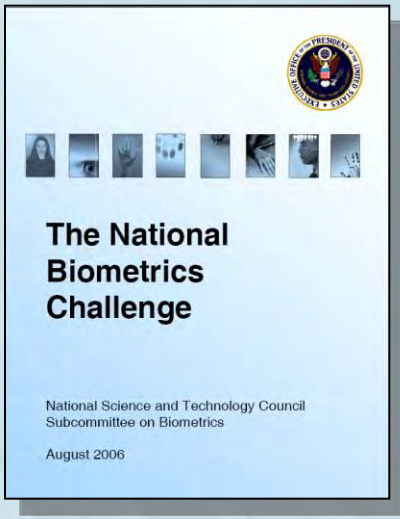
Homeland Security

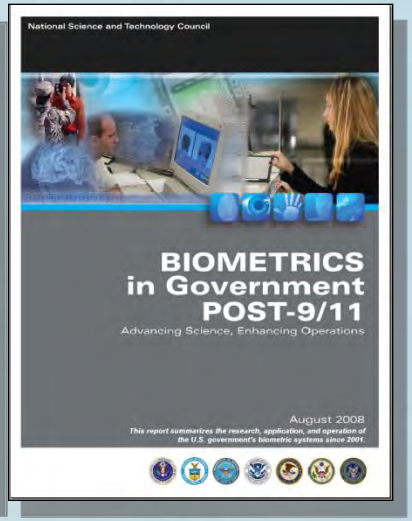
Indispensable Resources

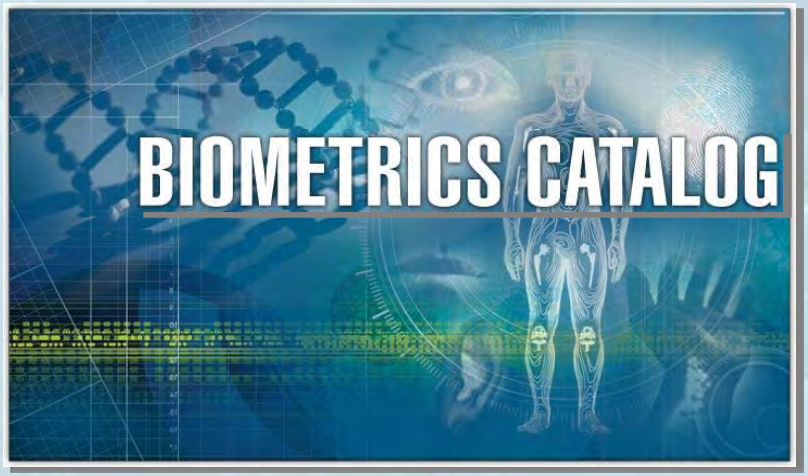
www.Biometrics.gov
- Central source on Federal government biometrics-related activities

www.BiometricsCatalog.org
- U.S. Government-sponsored database of public information about biometric technologies kept current by its users, who add information as it becomes available – Free to use and update

www.Biometrics.org
- Biometrics Consortium web site with free discussion bulletin board and annual conference news







Homeland Security

Homeland Security

Homeland Security

ID TECHNOLOGY PARTNERS

Biometrics: How do you know they work?

"Garbage in Garbage Out"

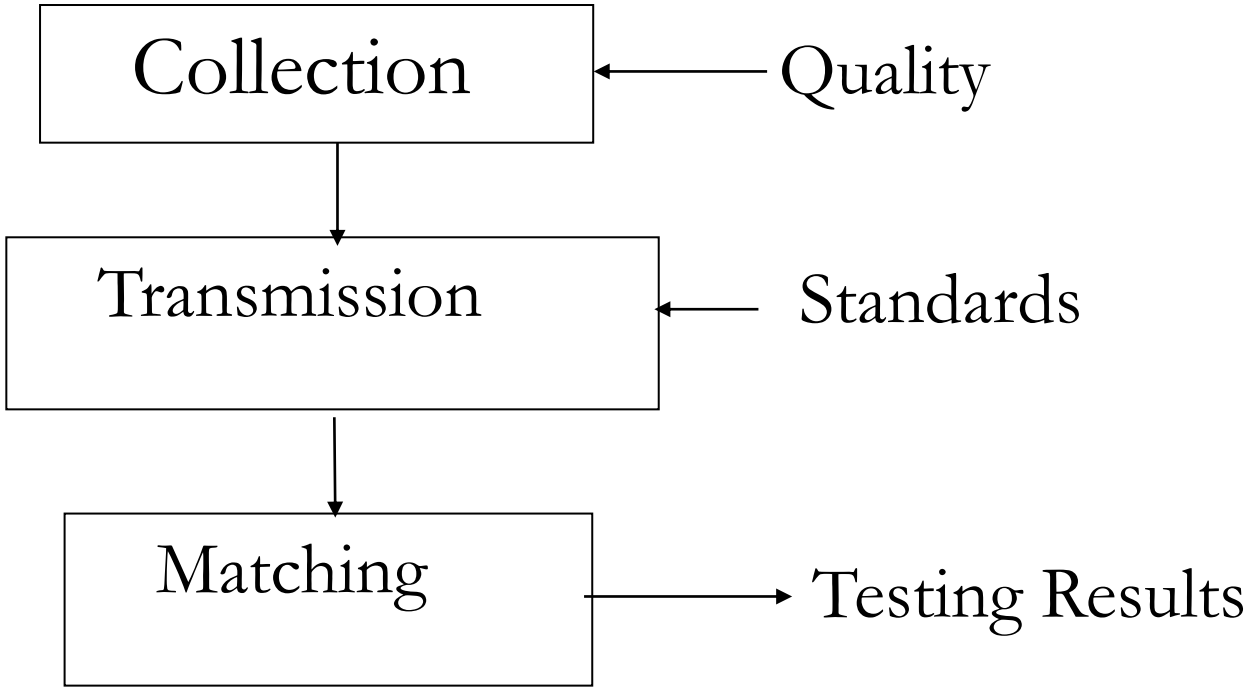
Conference & Technology Center
12 South Summit Avenue, Suite 110
Gaithersburg, Maryland 20877
301-990-9061

How do you know biometrics work?

ID TECHNOLOGY PARTNERS

- **Most biometrics work some of the time. If you never got a hit why bother?**
- **Both hits and misses are based on probabilities.**
- **You never know what your miss probability is unless you test.**
- **The testing process is well understood.**
- **To test you need a realistic test sample.**
  - –Big enough to get statistical numbers
  - –As close to your work load as possible
- **At every stage in the system quality is important. NIST Fingerprint Image Quality (NFIQ) is used here.**

Issues


Collection
Quality
Transmission
Standards
Matching
Testing Results

Topics

ID TECHNOLOGY PARTNERS

- **Standards**
- **Matching and Quality**
  - 10-finger Quality Measures
  - Difference in Transaction Used by the FBI
  - Accuracy is a Function of Quality
- **Standardization of System Testing**
  - Any AFIS could be setup to be tested .
  - This includes operational systems.
  - All that is needed is candidate lists with scores.
- **Multimodal Biometrics**
  - Usability - All biometric modes have image quality issues that are sensitive to acquisition procedures.
  - Fusion - How much would score level fusion improve biometric accuracy? How should it be done?

Standards

- **Standards needed for interoperability**
  - Ensure a high-level quality for captured images
  - Process fingerprints and other biometrics from dissimilar systems
- **Required types of standards**
  - Data format standards
  - Image quality standards
  - Performance standards
  - Conformance standards
- **Standards development organizations**
  - ANSI/NIST
  - M1/SC 37
  - Application Profile Interfaces (API)

ANSI/NIST–ITL Standard

- **Key transmission standard used by federal, state, & local law enforcement agencies**
  - FBI, DHS, PIV, DoD
  - De facto international standard (EURODAC, INTERPOL, UK, CA, etc.)
- **Updated versions developed to accommodate evolving biometrics and needs.**
- **A single standard used for the exchange of a subject's descriptive, demographic and biometric information**
- **Biometrics include fingerprint, face, iris, DNA, etc.**
- **Traditional and XML versions developed**
- **FBI EBTS 9.1 and DoD EBTS are 2.0 APIs based on standard**

MOBILE ID Devices

ID TECHNOLOGY PARTNERS

- Handheld or portable devices used to capture a subject's biometrics on the street, in a warzone, at a border, etc.
- Functions include enrollment, identification, and verification
- Applications include as physical/logical access control, border crossing, and checkpoint operations
- Capture and matching of biometrics in near real time with no transportation of subject and zero transit time
- Functions for enrolment, identification, & verification
- Best Practice Recommendation (BPR) lists progressively more stringent sets of image capture settings for the device
- BPR provides guidance on settings to be used based on function of device and risk to public safety.

CONFORMANCE

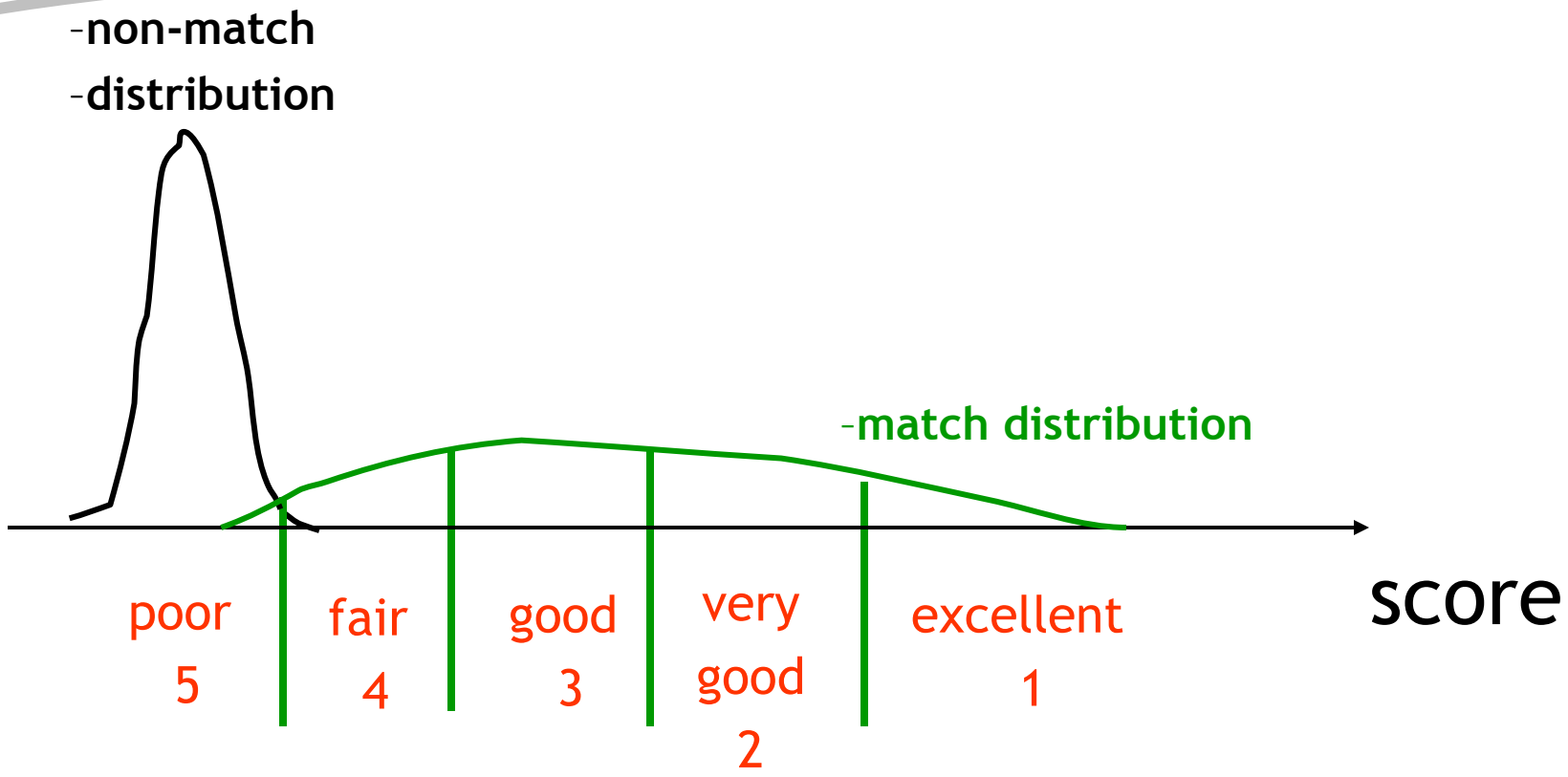
- **Data format conformance establishes confidence that an implementation fulfills the standard's requirements**
  - Syntactic conformance: correct structure, values, and bits for each field
  - Semantic conformance: faithful representation of captured biometric
- **Conformance requirements are part of the ANSI/NIST-ITL**
- **Hardware conformance**
  - FBI EBTS Appendix F specifies requirements for fingerprint live scan and field deployed mobile ID devices
  - Qualified products are listed on public website

Objective of NIST Fingerprint Image Quality (NFIQ)

ID TECHNOLOGY PARTNERS

- Define and develop a fingerprint image quality measure that can predict fingerprint recognition performance.
- Use ROC curves to check the quality of the new algorithm.

NFIQ Performance Score Prediction



Bin boundaries selected based on expected match score distribution

Analysis of FBI IAFIS Metadata

ID TECHNOLOGY PARTNERS

- This analysis took what was learned from many years of NIST tests and applied it to IAFIS performance
- Addressed quality issues
- Addressed the difference in quality between different subsamples and different TOTs (Types of Transactions)
- Addressed workload variation caused by quality

Sample Size Used in this work

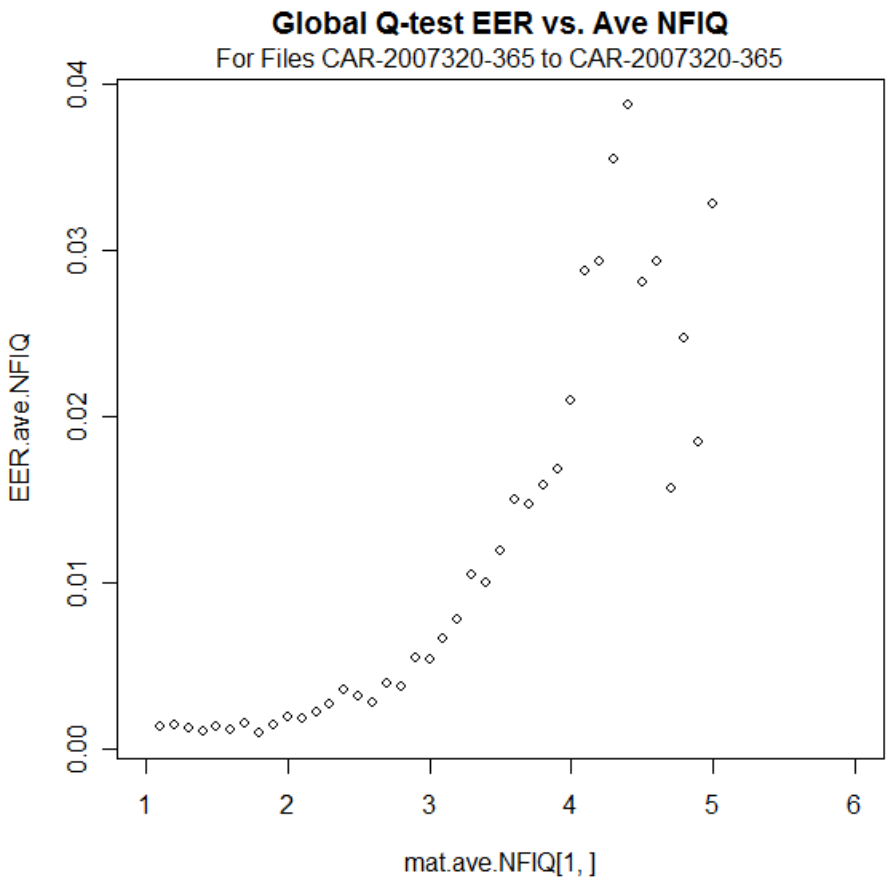
- All FBI submissions days between Nov. 11, 2007 and Dec. 31, 2008
- 45.9M samples, an average of 111K per Day
- Idents (valid Matches) 10.5M,
- Nonidents (No matches found) 28.9M
- 21.8GB of ASCII data
- Rolled
  - Idents 10.25M
  - Nonidents 15.63M
- Flat
  - Idents 309K
  - Nonidents 13.37M

10-Finger Quality Measures

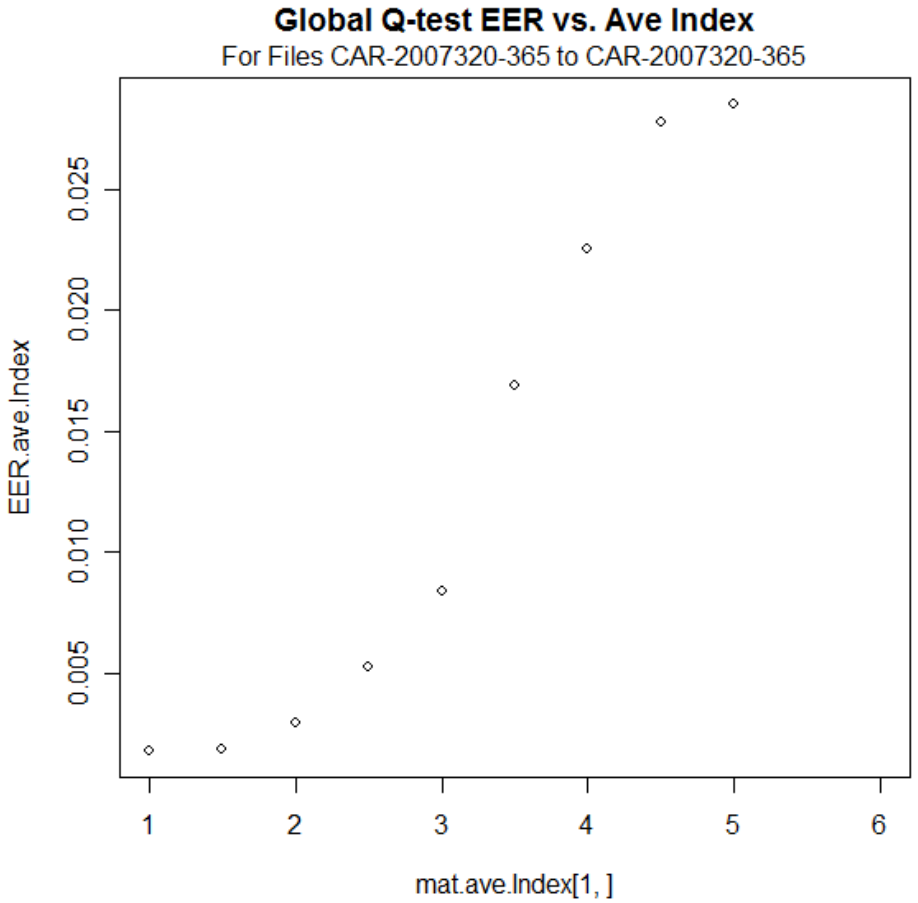
- **Seven different measures were tested**
- **Averages**
  - –All 10 fingers
  - –Index Fingers
  - –Average of 8
  - –Average of 6
- **Best N fingers of 10**
  - –Best of 5,4, or 3
- **Equal Error Rate (EER) is the point at which False Match Rate (FNR) equals the False Nonmatch Rate (FNMR)**

Equal Error Rate for Average of 10 Fingers and Index Fingers

10 Fingers



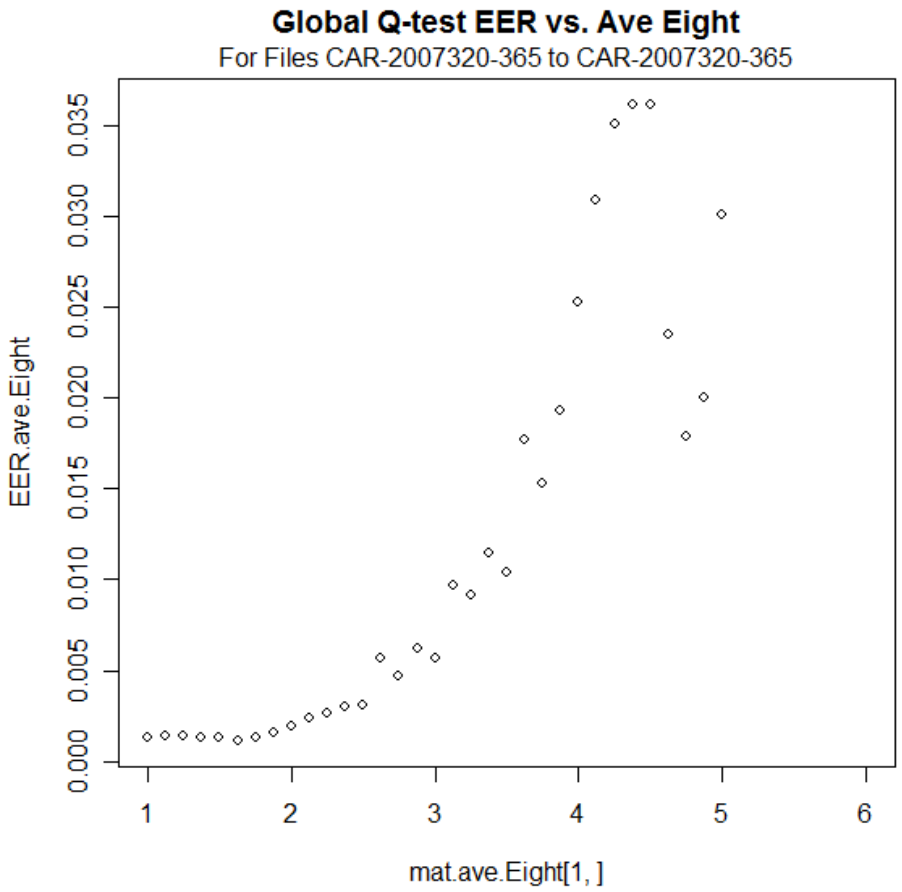
Index Fingers



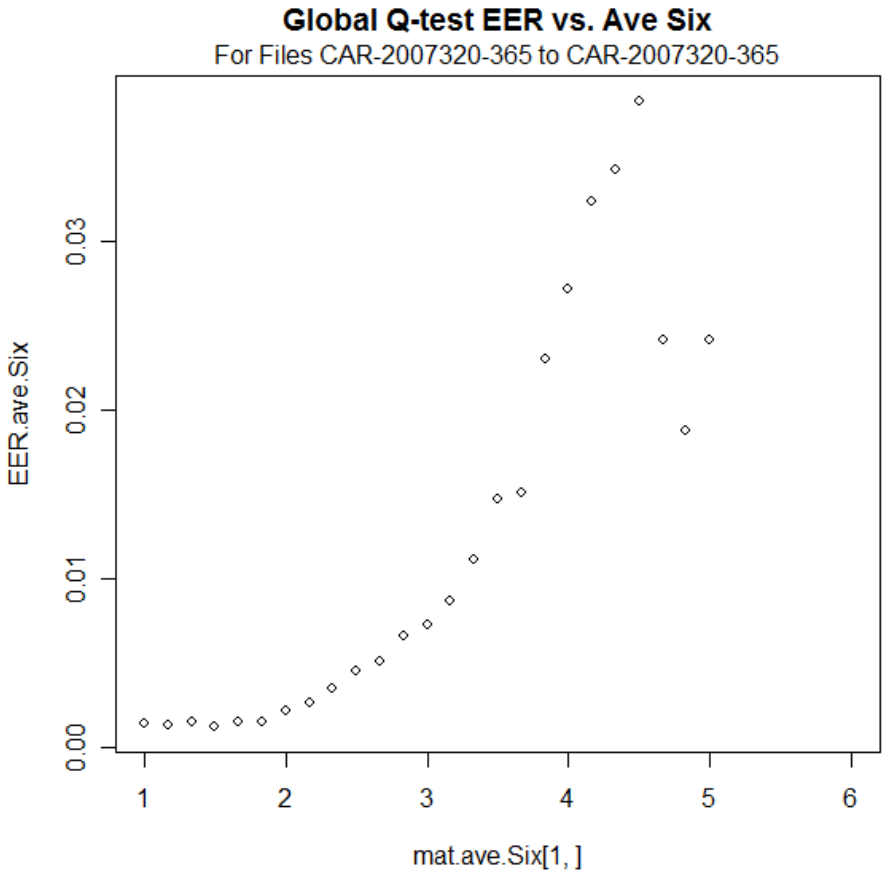
EER for Average of 8 and Average of 6

ID TECHNOLOGY PARTNERS

8 Fingers

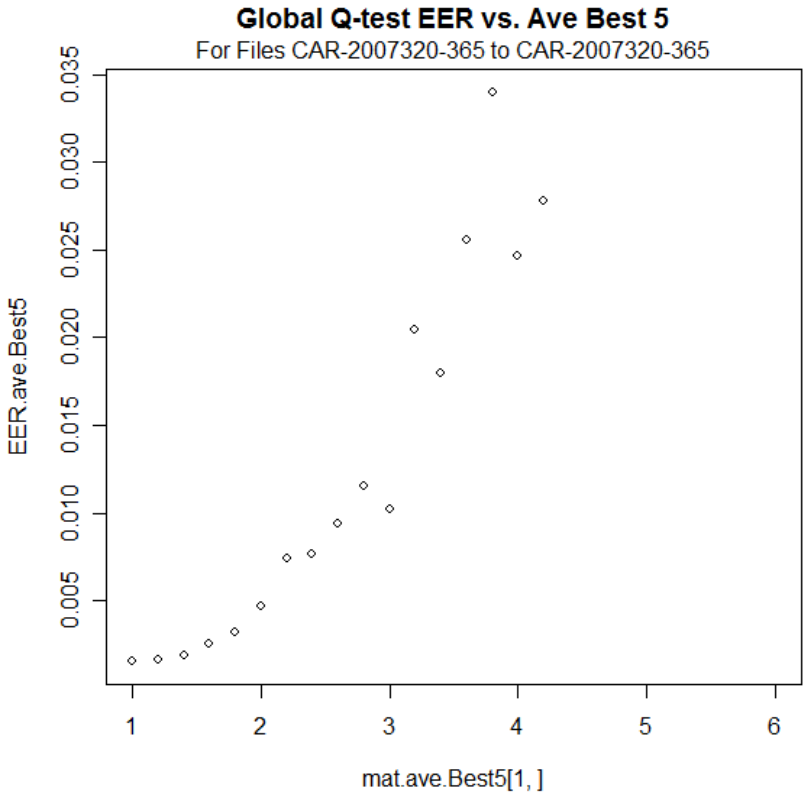


6 Fingers

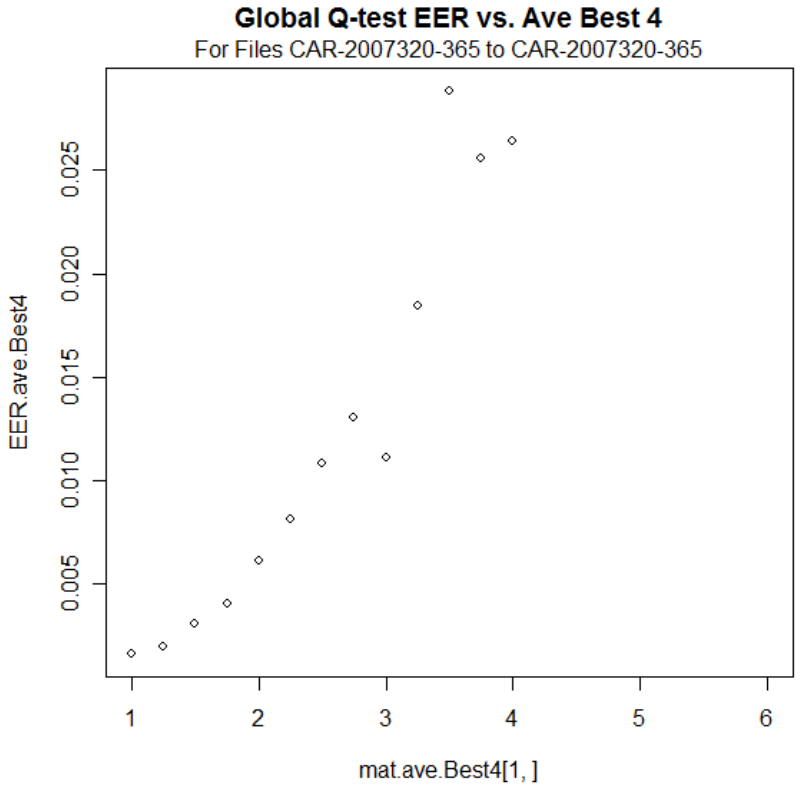


EER for Best 5 and Best 4

Best 5

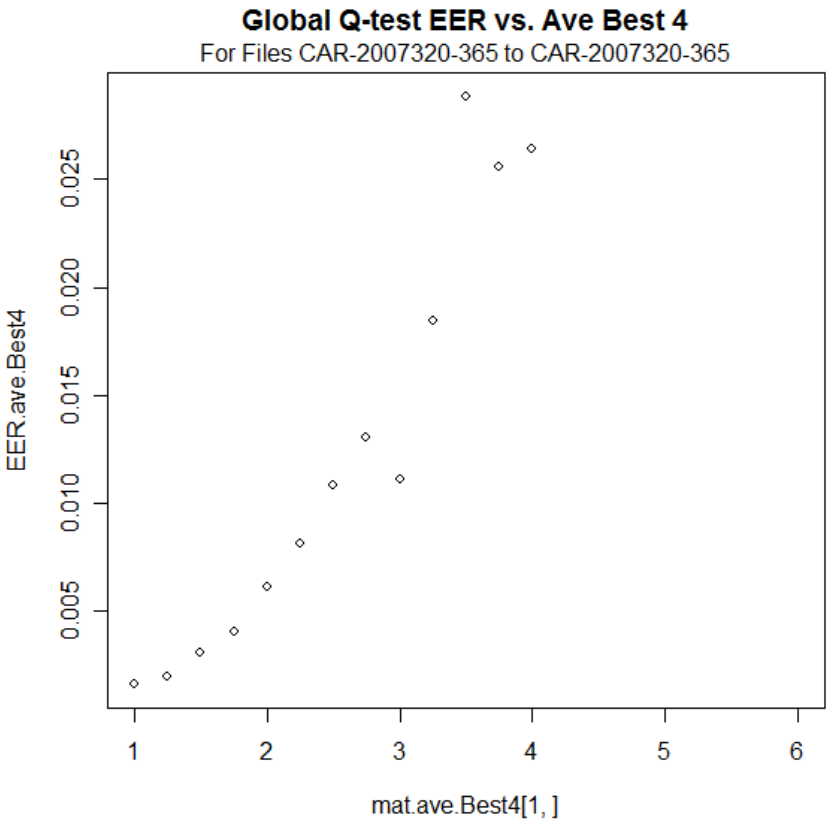


Best 4

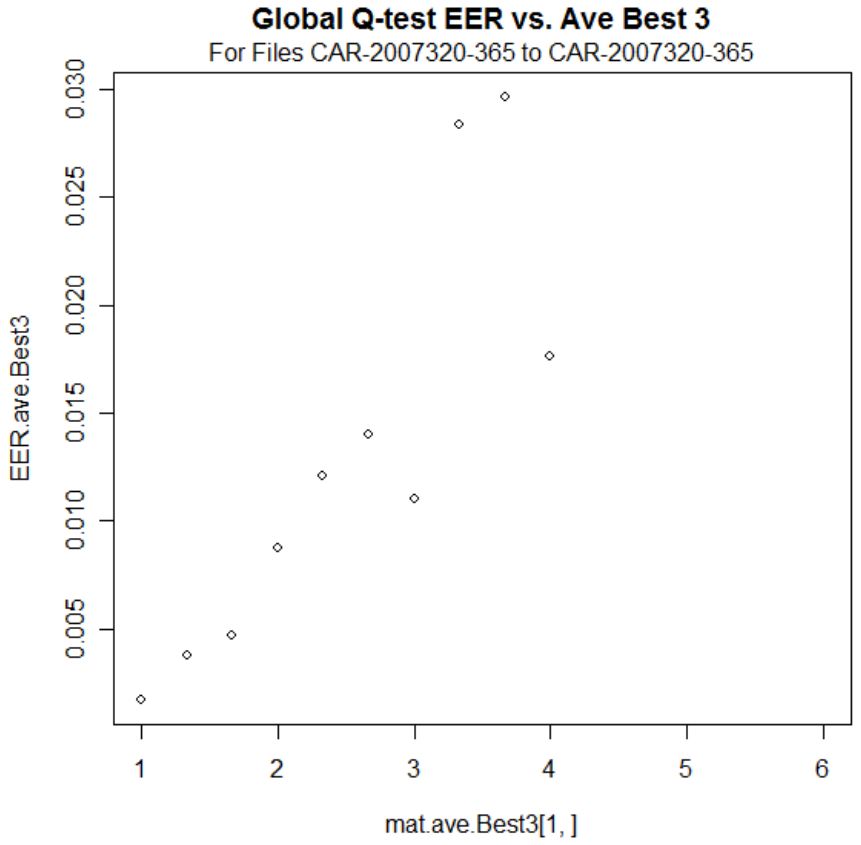


EER for Best 4 and Best 3

Best 4



Best 3



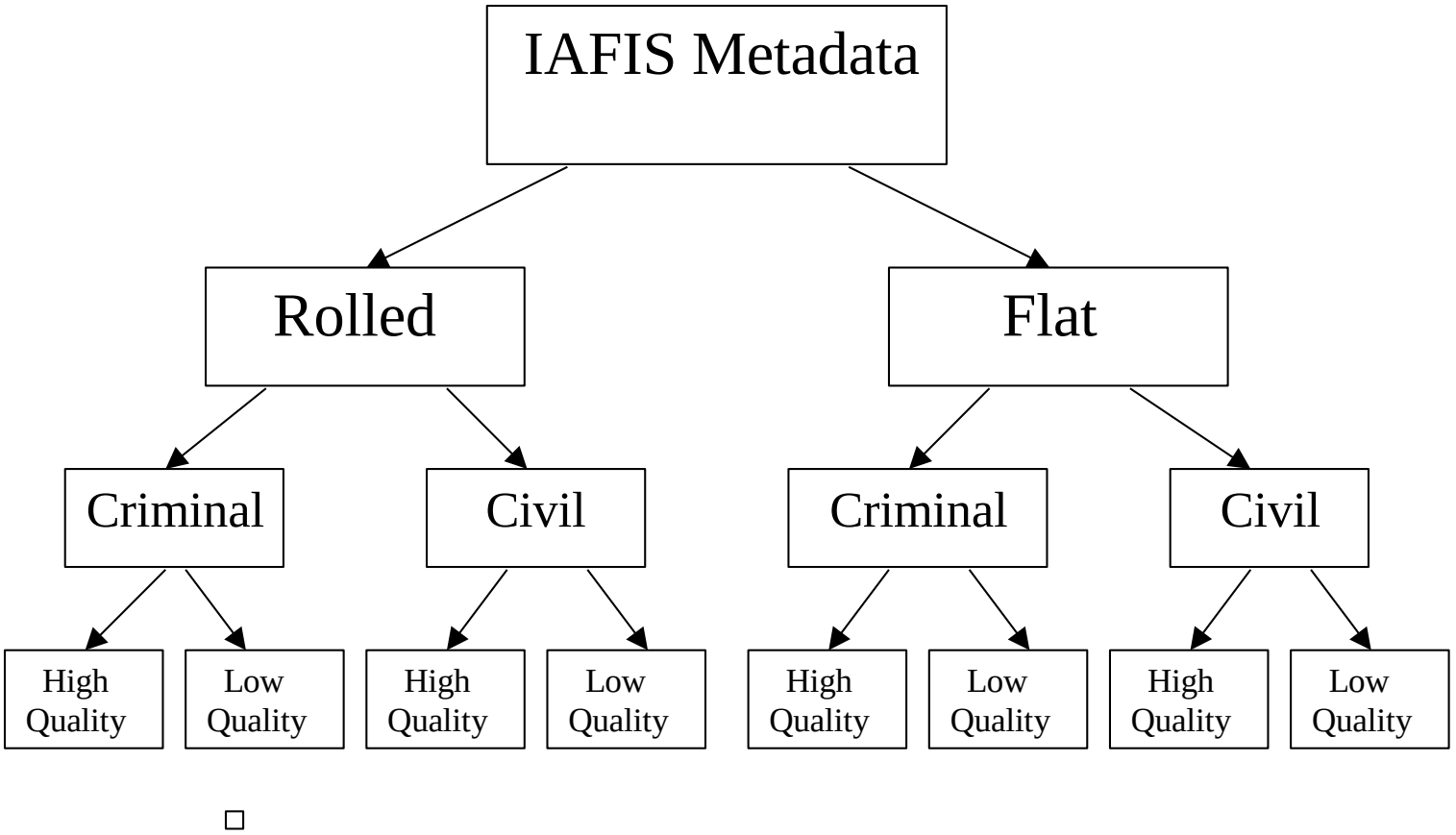
The Number of good fingers and the Quality Required for A Given EER Are Correlated

- **For a fixed 1% EER (Equal Error Rate):**
  - –Five finger require average NFIQ of 2.7
  - –Four finger require average NFIQ of 2.4
  - –Three finger require average NFIQ of 2.0
- **The fewer fingers you have the better they need to be for a given error.**
- **This test can be run on most operational systems.**

Average of 10-finger Works

- It is simple.
- It is fast – one line of code.
- It works well in the IAFIS application.
- Other measures can be used to get additional insight into system performance.

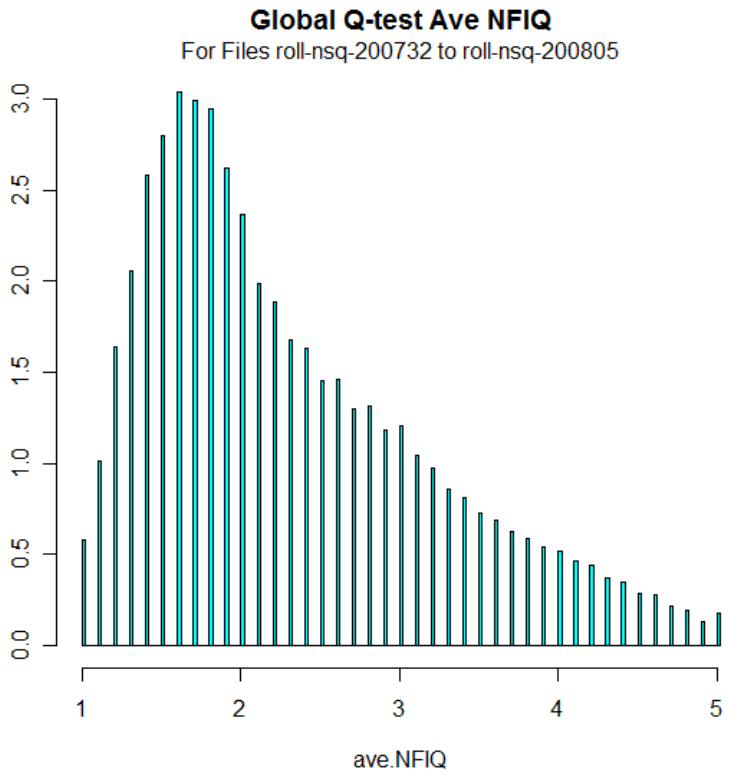
FBI Image Classes



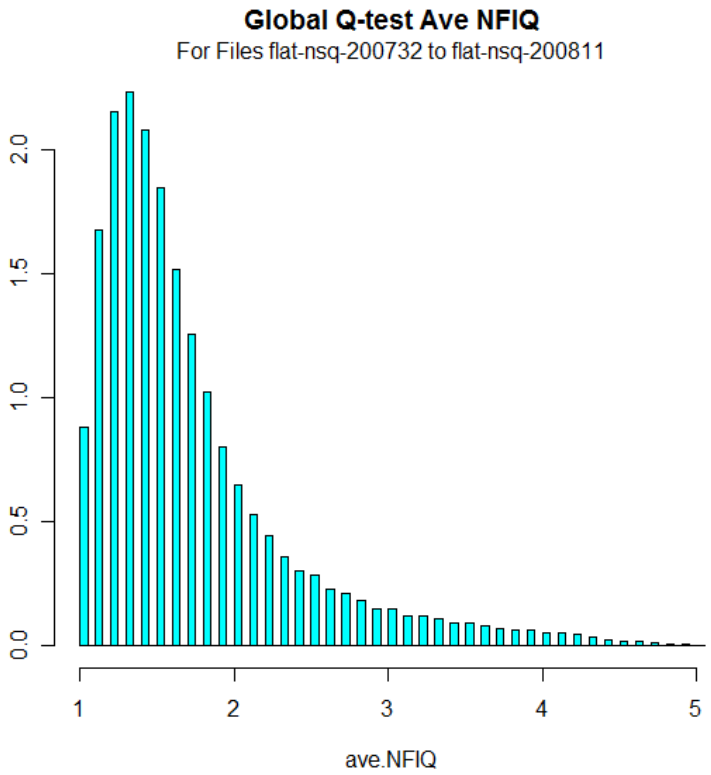
Each Image Class Has Different Quality

ID TECHNOLOGY PARTNERS

Rolled Verification Search



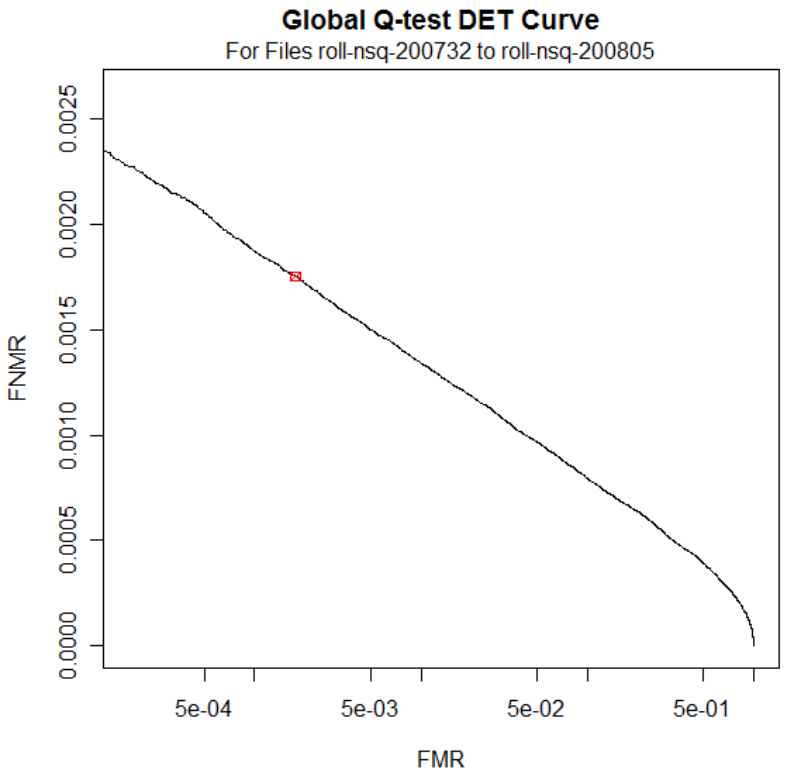
Flat Verification Search



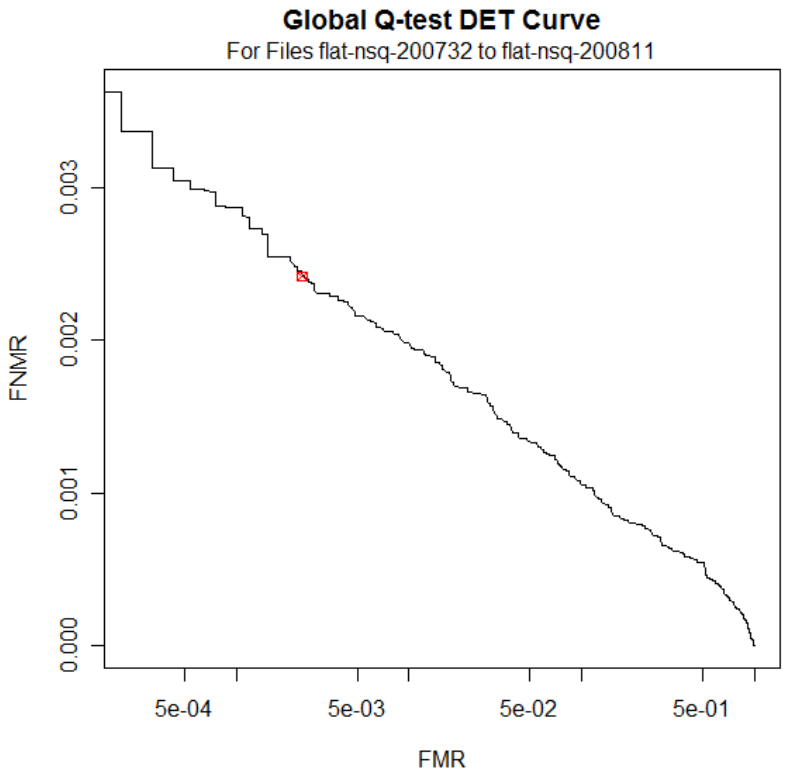
Each Dataset Has different March Accuracy

ID TECHNOLOGY PARTNERS

Rolled Verification Search



Flat Verification Search



These DETS show that flats are harder to match than rolled.

Error Rates Are Strongly Dependent on Quality

Type of Data	Equal Error Rate
Roll data	0.00175
Flat data	0.00242
Criminal data	0.0013
Civil data	0.0037
Criminal data quality1	0.00012
Criminal data quality5	0.011
Civil data quality 1	0.00023
Civil data quality 5	0.026

Transaction Analysis

ID TECHNOLOGY PARTNERS

- 10-finger average NFIQ can be used effectively to separate transaction types differences.
- The distribution of NFIQ values allows the fraction of difficult matches, NFIQ $\geq$ 4.2, to be evaluated.
- The difficult cases account for most of the missed cases.

Seven Transactions Dominate the FBI Workload

- Seven high-volume transaction account for 88% of the FBI IAFIS workload .
- 8.77% of the metadata items are for information requests or generate error responses.
- The seven transaction types which represent 1% or more of the work load represent 96.8% of all data items when information requests and errors are accounted for.

Quality of the Seven Major TOTs

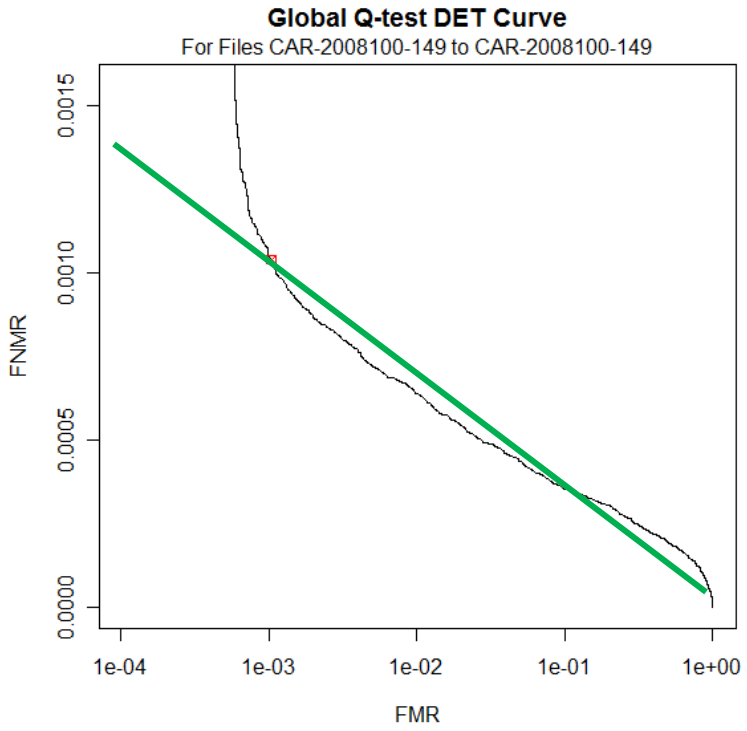
Transaction	Criminal-Civil	Flat-Rolled	Per Cent of Metadata	Average Daily Volume	10 finger Mean NFIQ	NFIQ 4.2 or Greater in Percent
CAR	Criminal	Rolled	26.69	29,000	1.95	3.00
NFUF	Civil	Flat & Rolled	28.08	34,600	2.00	5.21
NFUE	Civil	Flat	8.67	11,900	1.46	0.84
CPNU	Criminal	Flat	6.93	9,900	1.67	2.17
FAUF	Civil	Rolled	11.14	10,700	2.13	5.50
TPRS	Criminal	Rolled	4.16	4,800	1.85	2.15
FANC	Criminal	Rolled	2.36	2,300	2.04	3.87
			88.03	103,200		

Transactions using identical equipment get widely varying quality

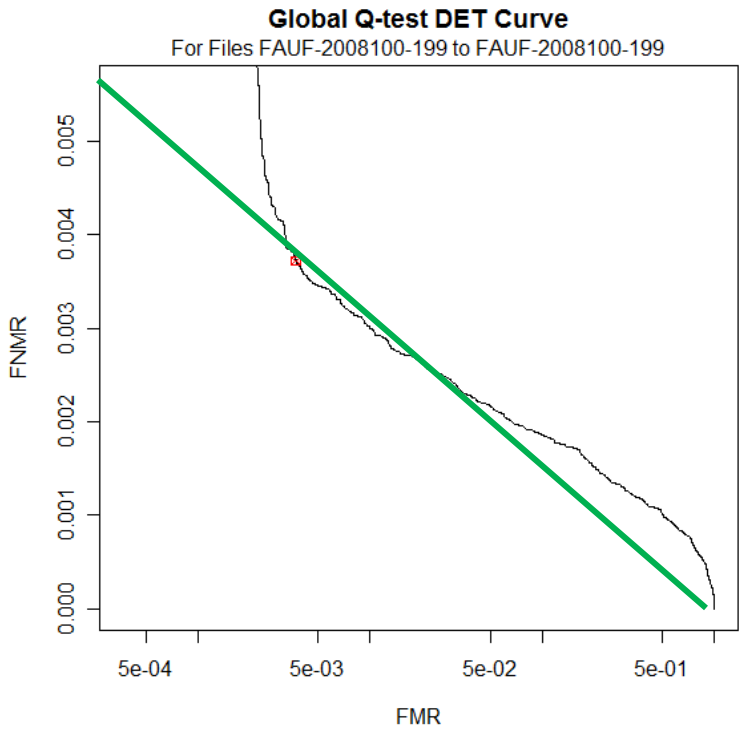
Each TOT Has a Different DET Curve

ID TECHNOLOGY PARTNERS

Criminal DET



Civil DET



Note the 3X difference in the scale of the errors.

Standardization of System Testing

ID TECHNOLOGY PARTNERS

- Any AFIS could be setup to be tested as IAFIS has been. This includes operational systems.
- All that is needed is candidate lists with scores.
- If this were done every match could return a probabilities on accuracy of hits and misses.
- This is the only way to know what is being missed.
- If search size equivalent information were available workload vs. quality can also be included

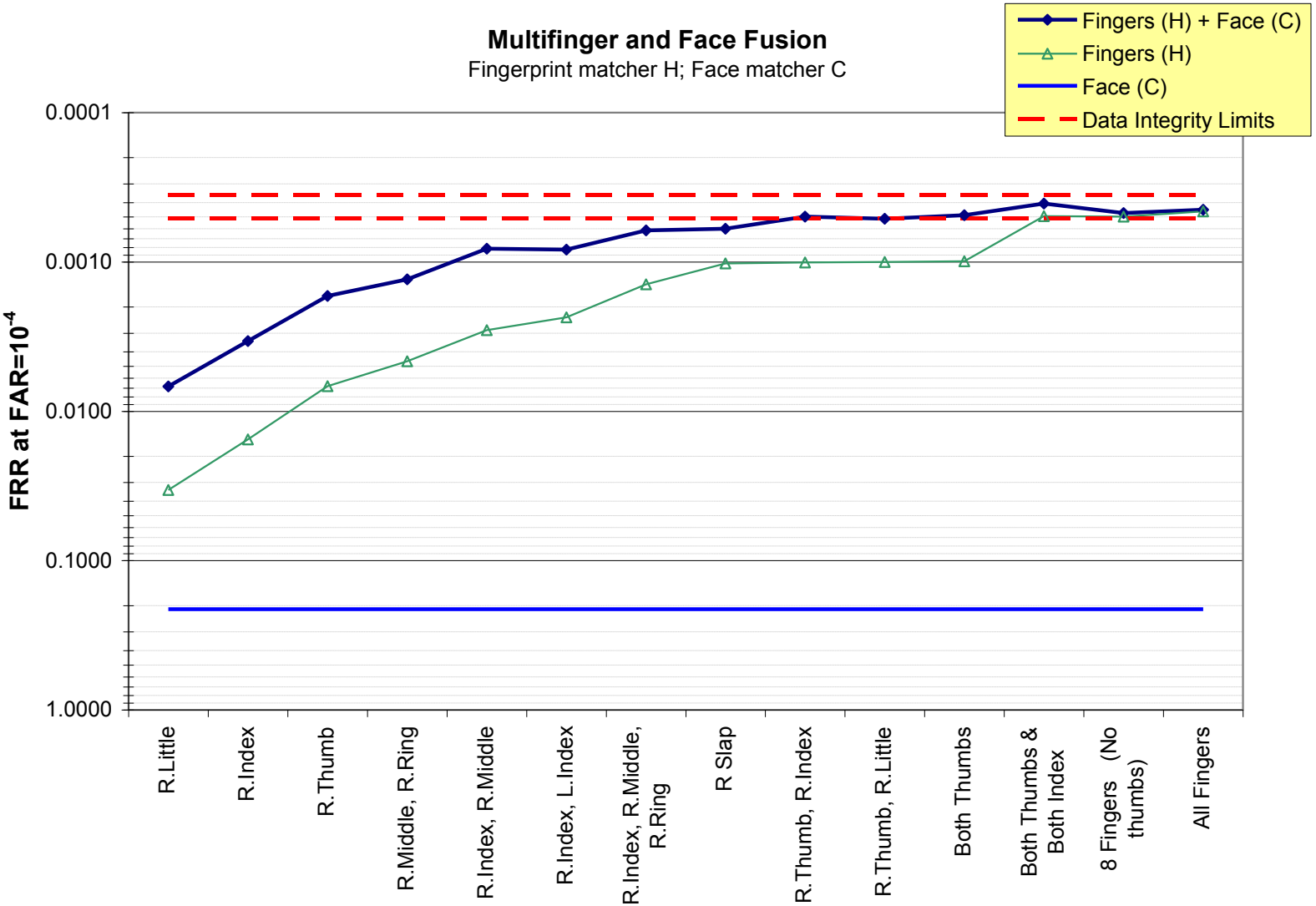
Multimodal Biometrics

ID TECHNOLOGY PARTNERS

- Usability - All biometric modes have image quality issues that are sensitive to acquisition procedures.

- How the match scores are combined is important. How much would score level fusion improve biometric accuracy? How should it be done?

Combinations of Fingers + Face



General Observations

- **Whether the benefits of fusion can be realized in practice depends on**
  - Availability of multi-biometric data and/or multiple matchers
  - The accuracy of the matchers
  - The correlation of the scores
  - Sample similarity and quantity of training data

Current Status

ID TECHNOLOGY PARTNERS

- Testing has barely scratched the surface of multimodal applications.
- Relatively simple methods can provide significant accuracy gains.
- Lack of correlation between biometric modes should be tested not assumed.

Conclusions

- **Garbage in Garbage Out**
  - –Very low quality data sharply reduces hits and increases misses
  - –Low and high quality data have sharply different matching characteristics
- **It can be improved.**
  - –Better input quality means more hits and fewer misses
  - –Multimodal matching can improve accuracy.

Contact Information

Charles Wilson

ID Technology Partners, Inc.

12 South Summit Avenue

Gaithersburg, Maryland 20877

301-527-1232 (Direct Phone)

301-990-9062 (Direct Fax)

cwilson@idtp.com

WEB: www.idtp.com

America Identified
MIT Press, 2010

Lisa S. Nelson J.D., Ph.D.
Graduate School of Public and International Affairs
University of Pittsburgh

Societal Impact Study: Scope

- National Science Foundation Study
- 100 person pilot study: Testing the Survey Design
- 1,000 Random Digit Dial Survey: General Societal Perceptions
- Focus group research of non-end users and end users of biometric technology

Focus Group Research

- Eight Focus groups were conducted in November 2005 through July of 2006 with the assistance of American Institute for Research.
- Four focus groups of non-end users were conducted to address the issues of privacy, civil liberties, and psychological and cultural responses to various types of biometric technology in a variety of settings to gauge the parameters of societal acceptance
- Four focus groups were conducted to address similar issues with current end users of biometric technology in a variety of settings including governmental, banking, and business.

National Survey

- 1000 Person National Survey
- The issues of privacy, civil liberties, data protections, different potential uses of biometric technology and general perceptions of data sensitivity addressed on a national scale.

Focus Group Topics

- Privacy of personal information.
- Institutions and their handling of private information.
- Biometric technology as a way to protect private information.
- Situations where the use of biometric technology is acceptable.

Privacy

- Legal guarantees
- Normative concerns
- Protecting privacy in institutions?
- Considerations?

Decisional Autonomy: Privacy in Public

- Concerns
- Limitations on surveillance of mobilities
- Policy: limitations of use, protection of biometric information, privacy notices

Trust and Confidence in Institutions

- Which institutions illicit increased trust and confidence in handling of information?
- Why?
- Medical and Financial sectors are most highly rated because of HIPAA and GLB
- Implications for biometric identifiers

Paternalism and Objectives

- The meaning of paternalism in democracy
- Choice is not always liberty
- When paternalism is acceptable
- Directives for policy

The Parameters of Societal Acceptance

- Normative Dimensions of Privacy
- The Role of Institutional Confidence and Trust
- Paternalism
- Purpose of the Personal Information relative to Policy Objective
- Information as currency
- The place for Biometric Technology





The Center for Identification Technology Research (CITeR)

Presented by Dr. Stephanie Schuckers
February 24, 2011

Clarkson UNIVERSITY defy convention

CITeR Status Report

CITeR is an NSF Industry/University *Cooperative* Research Center (IUCRC)

– The importance of individual identity in a networked global society

– Research cooperatively defined, funded and shared

– Scope: Physiological, Behavioral, and Molecular Biometrics

- ***2001: WVU Founding Site***, MSU Partner, 5 Founding Affiliates
  - Automated Biometric Recognition
- ***2006: University of Arizona becomes 2nd Site***, 10+ Universities
  - Credibility, psychophysiological and behavioral deception detection
- ***2010: Clarkson Plans 3rd Site***, over 20 Affiliates plus 9 Prospective
  - Logical and cyber identity, intelligence

CITeR Cooperative Model

CITeR Current and Committed Affiliates

Clarkson UNIVERSITY

- Accenture
- Booz Allen Hamilton
- Computer Science Corporation
- DIA/DACA-Defense Academy for Credibility Assessment
- Department of Defense—Biometric Task Force
- Department of Defense—DDR&E
- Department of Defense—USSOCOM/SOALT
- Department of Homeland Security—S & T 3 memberships (1 Clarkson)
- BORDERS DHS COE
- Federal Aviation Administration, Information Systems Security (2 memberships)
- Federal Bureau of Investigation
- Irvine Sensors
- Laurea Ltd.
- Lockheed Martin
- National Institute of Standards and Technology (NIST)
- National Security Agency 2 organizations (1 Clarkson)
- Northrop Grumman
- OU Center for Applied Social Research
- Raytheon (2 organizations)
- Morpho Trac Inc.
- Sandia National Labs
- SRC
- Science Applications International Corporation (SAIC)
- US Army Picatinny Arsenal
- US Army CERDEC/SBInet Indep. Test Team
- West Virginia High Technology Consortium Foundation

Booz | Allen | Hamilton

Raytheon

Homeland Security

SAIC

accenture

Federal Aviation Administration

WVHTC FOUNDATION

UNITED STATES SPECIAL OPERATIONS COMMAND

CSC EXPERIENCE. RESULTS.

National Security Agency Central Security Service

LOCKHEED MARTIN We never forget who we're working for

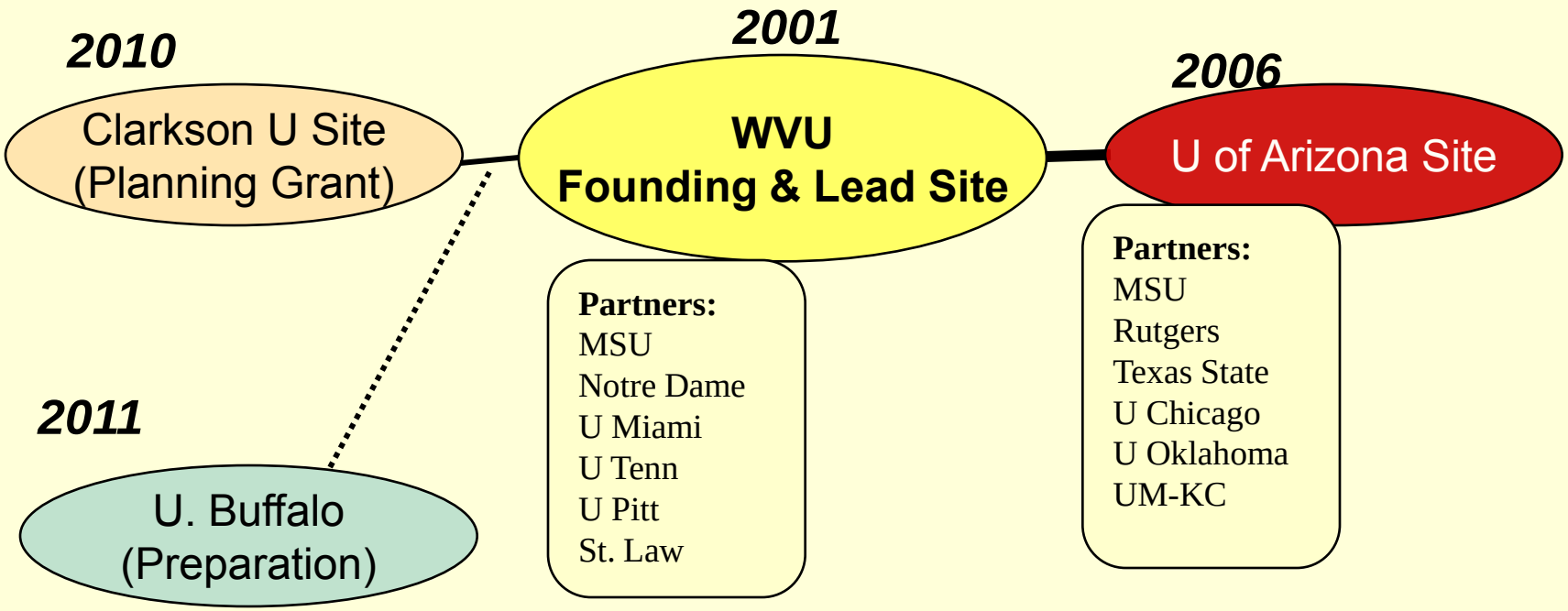
Defense Research & Engineering Innovation, Speed and Agility

MorphoTrak SAFRAN Group

NORTHROP GRUMMAN DEFINING THE FUTURE

Multi-University Trajectory

CITeR has grown its participating faculty and university site partners to stay at the leading edge of biometrics & meet affiliate needs.

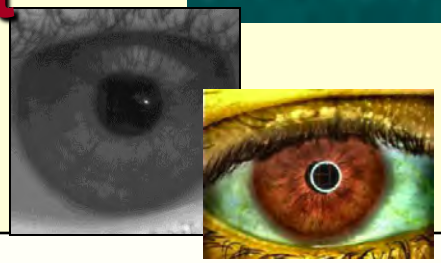


Prior Research Portfolio Snapshot

Clarkson UNIVERSITY

Fingerprint
- Level 3
- Liveness
- Anonymous biometrics
- Biometric cryptosytems
- Quality

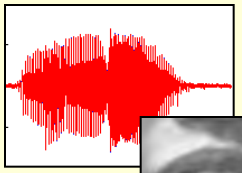
Palmprint
- Level 1,2,3
- Partial

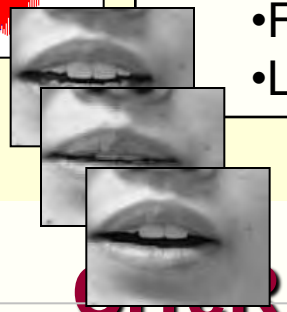


Iris
- Non-ideal, off angle
- Unconstrained
- Iris at a distance
- Multispectral
- Quality

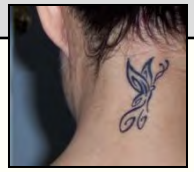
Credibility
- Kinesic
- Audio
- Linguistic

Multimodal
- Fusion score/feature level, quality
- Indexing
- System level design & evaluation
- Sensor networks
- Statistical performance evaluation

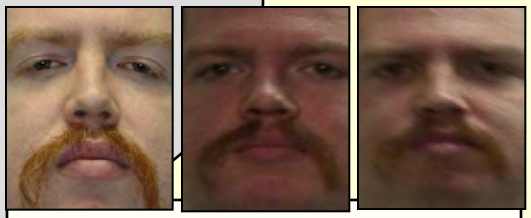




Voice
- Fusion
- Lip



Others
- Gait
- Conjunctival vascular
- Tattoo, body markings
- Soft biometrics
- Age progression

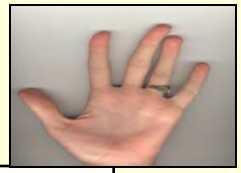


Face
- Matching, quality
- Unconstrained
- 3D Face
- Face in a crowd

Future Research Directions

Clarkson UNIVERSITY

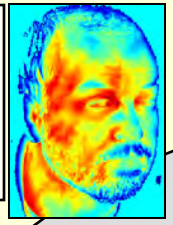
Fingerprint



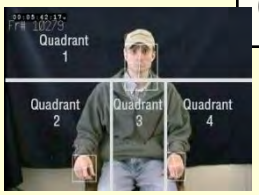
Palmprint

Iris

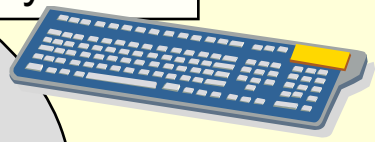
Trust
- Suspicion
- Health



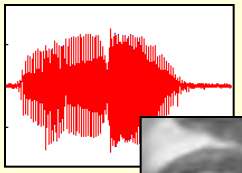
Credibility



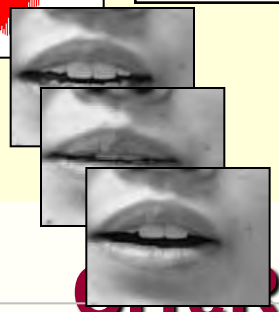
Cyber-Identity
- Logical
- Keystroke



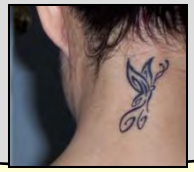
Multimodal
- Non-cooperative, distance biometrics
- Intelligence and biometrics
- Fusion with voice
- Fusion with liveness
- Scalability, individuality

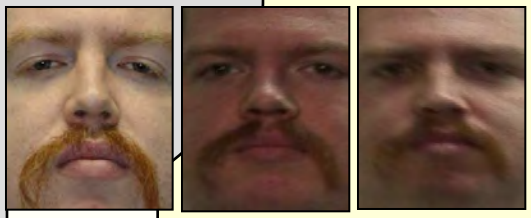


Voice



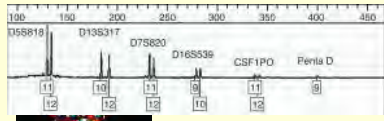
Others



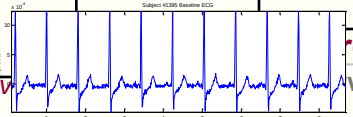


Face

Molecular
- DNA
- VOC



Cardiorespiratory
- Uniqueness
- Distance



Summary of Major Outcomes & Impact

- **Books:**
  Schuckers, Computational Methods in Biometrics: Statistics for Performance Evaluation , Springer, 2010.
  Nelson, America Identified: Society and Biometric Technology,, MIT Press, 2010.
  Maltoni, Maio, Jain, Prabhakar, Handbook of Fingerprints, 2nd Edition, Springer 2009.
  Jain, Flynn, Ross, Handbook of Biometrics, Springer, 2007.
  Ross, Nandakumar, Jain, Handbook of Multibiometrics, Springer Verlag, 2006.
  Li, Jain (Eds.), Handbook of Face Recognition, Springer Verlag, 2005.
- **Public dataset:** Public releases of large multi-modal datasets
- **National Survey Conducted:** Illuminating biometric acceptance in DHS context
- **Software:** MUBI CITeR's multibiometrics fusion analysis and CITeR's PRESS used by DHS, others
- **M1 Leadership in multibiometric fusion**
- **Port-of Entry Study:** Predictive analysis of biometrics, MRTD impact
- **Over 100 publications to date**
- **Over 20 Master's/Ph.D. students graduated to date**
- **Technology transfer:** Fingerprint liveness algorithms, successful small business development funding

CITeR Research Portfolio 2011

- Heterogeneous Face Recognition
- Generalized Additive Models for Biometric Fusion and Covariate Analysis
- Feasibility Study of an International Biometrics Data Portal
- Facial Metrology for Human Classification
- LivDet II Fingerprint Liveness Detection Competition 2011
- Post Mortem Ocular Biometrics Analysis
- A Standardized Framework for a Heterogeneous Sensor Network for Real-Time Fusion & Decision Support
- Comparison of Methods for Identification & Tracking of Facial & Head Features Related to Deception & Hostile Intent
- Establishing Deceptive Behavior Baselines for Eye-Tracking Systems

Research Portfolio 2010

- A Study of MWIR for Face Recognition & Liveness
- Cross-Age Face Recognition Based on a Facial Age Estimation Scheme
- Enhancement & Quality Assessment Schemes for Challenging DNA Analysis
- Optimizing the Design of Large Scale Biometric Security Systems
- Latent Fingerprint Enhancement
- Dyadic Synchrony as a Measure of Trust & Veracity
- Improving Information Security through Authentication Technology
- Temporal Alignment of Psychophysiological Behavioral Indicators
- Non-cooperative Biometrics at a Distance
- Iris Segmentation Quality Analysis: Prediction and Rectification
- Impact on Age & Aging on Iris Recognition
- Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters
- Detecting, Restoring & Matching Altered Fingerprints
- SPLICE: Integrating Agent99, LIWC & Building an Accessible
- Identifying Hidden Patterns from Facial Expressions
- Animating the Automated Deception Analysis Machine (ADAM)
- Automatic Deception Systems: To Believe or Not to Believe

BIMA
BIOMETRICS IDENTITY MANAGEMENT AGENCY

National Defense Industrial Association Biometrics Conference Roadmap to Tomorrow

23 February 2011

Dr. Thomas Killion

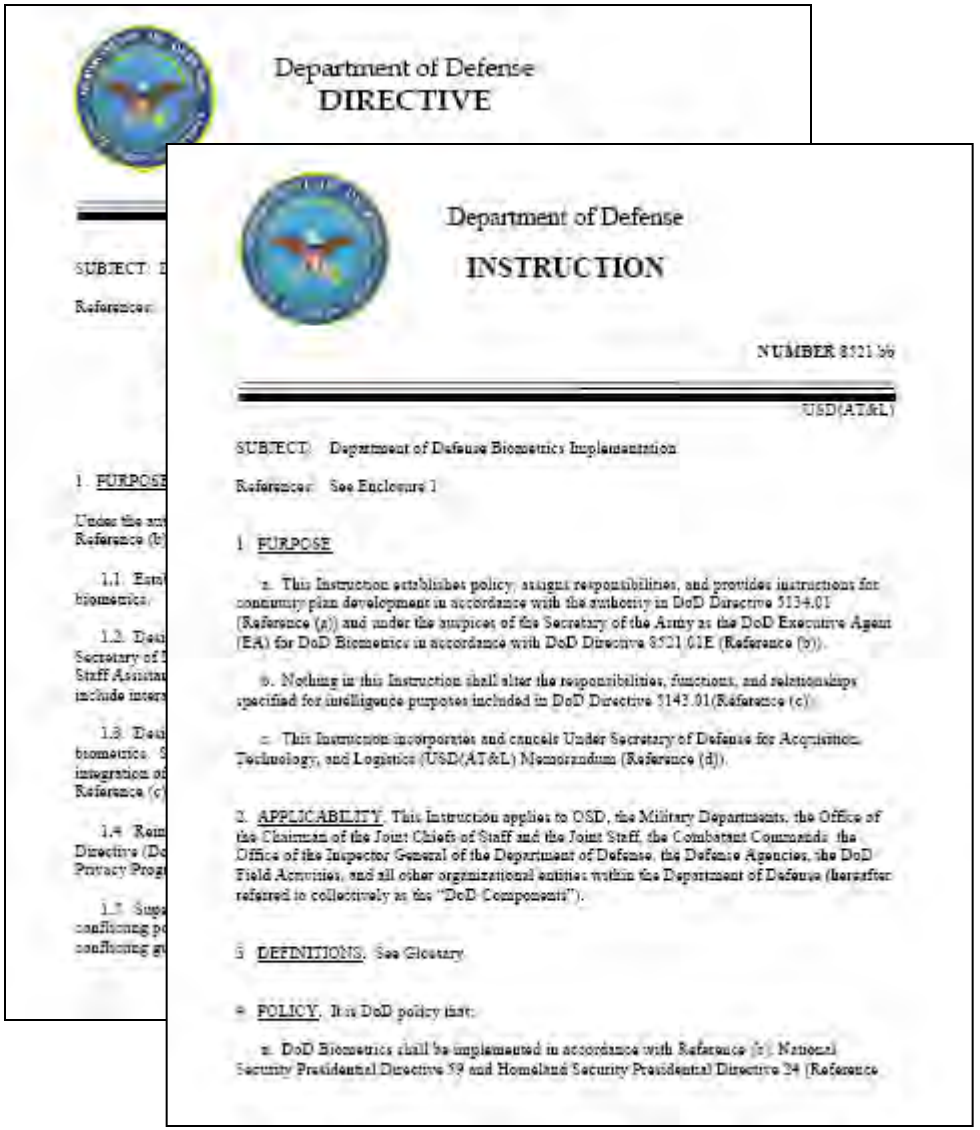
BIMA Vision

Vision: Protect the nation through the employment of Biometrics capabilities

The DoD Biometrics Enterprise

Key Players

- OSD
  - DDR&E (PSA)
  - DDB
- HQDA
  - G-2
  - G-3/5/7
  - G-6
  - ASA (ALT) (PEO-EIS)
- Joint Staff
- Services
- COCOMs
- OPMG
- TRADOC Capabilities Manager Biometrics & Forensics



Department of Defense
DIRECTIVE

SUBJECT:

Department of Defense
INSTRUCTION

NUMBER 8521.99

USD(AT&L)

SUBJECT: Department of Defense Biometrics Implementation

References: See Enclosure 1

1. PURPOSE

a. This Instruction establishes policy, assigns responsibilities, and provides instructions for community plan development in accordance with the authority in DoD Directive 5134.01 (Reference (a)) and under the auspices of the Secretary of the Army as the DoD Executive Agent (EA) for DoD Biometrics in accordance with DoD Directive 8521.01E (Reference (b)).

b. Nothing in this Instruction shall alter the responsibilities, functions, and relationships specified for intelligence purposes included in DoD Directive 5143.01(Reference (c)).

c. This Instruction incorporates and cancels Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L) Memorandum (Reference (d)).

2. APPLICABILITY. This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. DoD Biometrics shall be implemented in accordance with Reference (e), National Security Presidential Directive 59 and Homeland Security Presidential Directive 24 (Reference

Institutionalizing Biometrics

Rapid Acquisition

- Urgent Needs (JUONS, UONS)
- Integrated Rapid Fielding
- Sustainment

Urgent Capabilities

ABIS
BAT-A (w/ refresh)
HIIDE
BISA
SEEK

If need is Persistent

Deliberate Acquisition

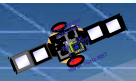
- Requirements (JCIDS)
- Planning, Programming, Budgeting and Execution (PPBE)
- Defense Acquisition System (DAS)

BEC – Milestone B, 4Q FY 12
JPI v2 – Milestone B, 4Q FY 12
IDS – FY 14+

Program of Record

Biometrics Process in Support of DoD Operations

BIMA BIOMETRICS IDENTITY MANAGEMENT AGENCY



Global Communications

Biometric Modalities

- Fingerprint
- Iris
- Face
- Palm
- DNA
- Voice
- Future Modalities

Collect

Manage

Store

Match

Share

Analyze/Reference Data

Decide Act

Operational Applications

- Populace Management
- Force Protection
- Access
- Surveillance
- Monitoring
- Combat ID

Maritime Interdiction Vessel

Military Operations and Business Functions

DoD ABIS Overview

- DoD ABIS online July 2004 (fingerprints only)
- DoD NG ABIS online 30 January 2009 (multi-modal)
- Stores and matches fingerprint, iris, face, and palm modalities

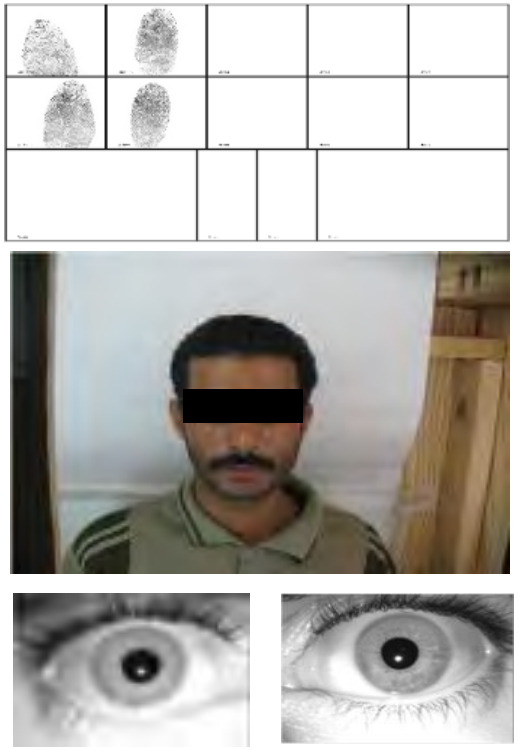
- 3,800+ transactions per day; rated for 8,000
- 4.2M records rated capacity
- Greater operational capability
  - Single or multi-modal processing
  - Expandable to process additional modaliti
  - 95% lights-out matches
  - Latent to latent searches
    - 120k latent fingerprints
    - 8600 latent matches; 3400 latent to latent matches
  - Latent palm print capabilities

- During data migration from ABIS to NG-ABIS, observed 10% new matches the previous system missed

Multi-Modal Biometric Fusion

Multi-modal biometric fusion (currently only DoD ABIS) results in:

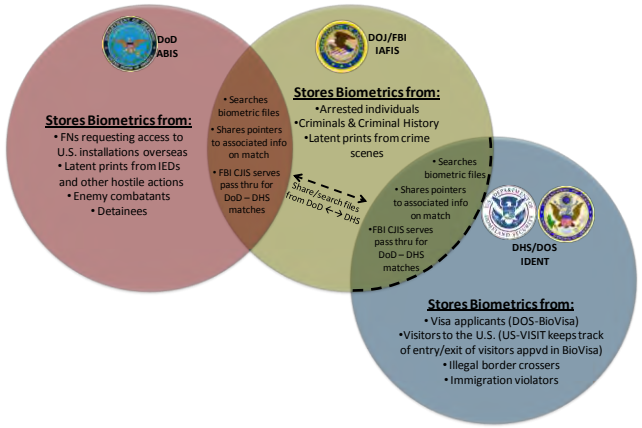
- **More matches through the correlation of other modalities**
- **More auto-identification, with lower number of manual examinations required**
- **Improved overall system accuracy and performance**



The fusion algorithm combined near matches to identify the individual.

Interagency Data Sharing

Current State



Desired End State

DoD ABIS

DOJ/FBI IAFIS

Stores Biometrics from:
- FNs requesting access to U.S. installations overseas
- Latent prints from IEDs and other hostile actions
- Enemy combatants
- Detainees

- Searches biometric files
- Shares pointers to associated info on match

Stores Biometrics from:
- Arrested individuals
- Criminals
- Latent prints from crime scenes

Action:
- Prosecute/Exonerate
- Allow/Deny Access
- Detain/Release
- Add to/remove from watch list

- Searches biometric files
- Shares pointers to associated info on match

- Searches biometric files
- Shares pointers to associated info on match

Stores Biometrics from:
- Visa applicants (DOS-BioVisa)
- Visitors to the U.S. (US-VISIT keeps track of entry/exit of visitors approved in BioVisa)
- Illegal border crossers
- Immigration violators

DHS/DOS IDENT

Areas for Expansion

- New Modalities – Voice, Gait, Ear Shape, etc
- Enhanced Capabilities
  - Facial Image Based Meta Data
  - Digitally-signed forensics images
  - Matching Algorithm
- New Domains
  - Friendly Biometrics (IDProTECT)
  - Defining New DoD Requirements
  - Addressing the Policy Considerations within new domains

Biometrics is an ENDURING CAPABILITY

Even after the completion of Overseas Contingency Operations, Biometrics will remain an enduring capability that enables DoD Stakeholders to execute their missions.

- **Biometrics will continue to support the Warfighter across the range of military operations**
- **Biometrics capabilities will grow to enable operations in new and evolving mission areas**
- **DoD Biometrics will expand our relationships and interaction with Interagency Partners**

Questions

Building an area of area of freedom, security and justice

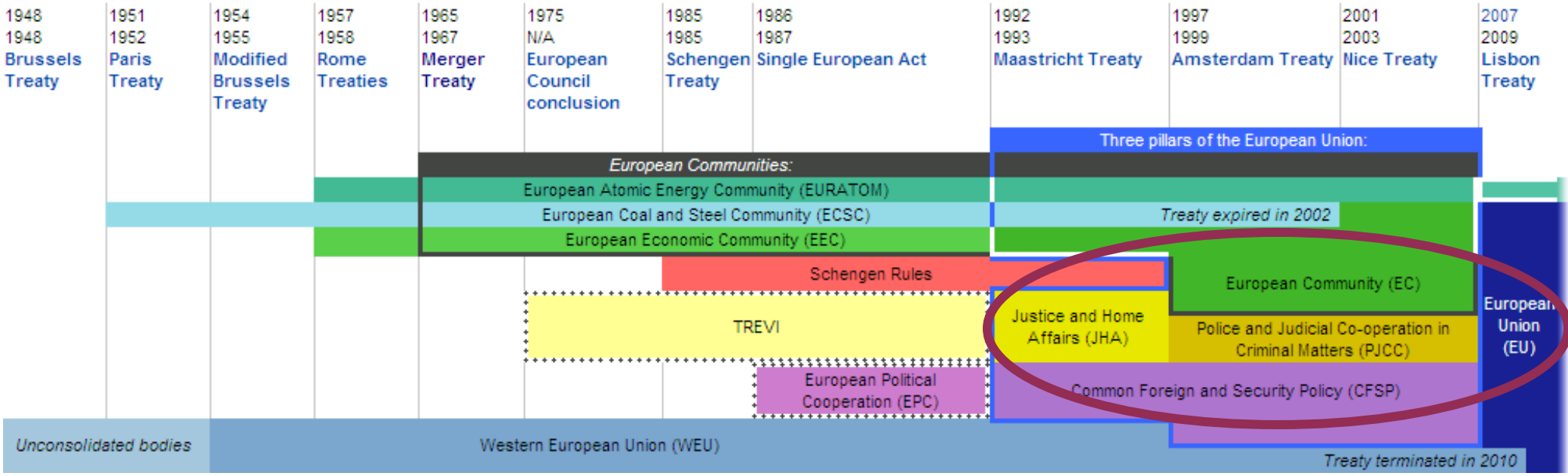
…exchanging biometric data in the EU…

Gillian Ormiston
Global Market Manager for Border Solutions

SAFRAN
Morpho

Understanding the European Union

an area of freedom, security and justice

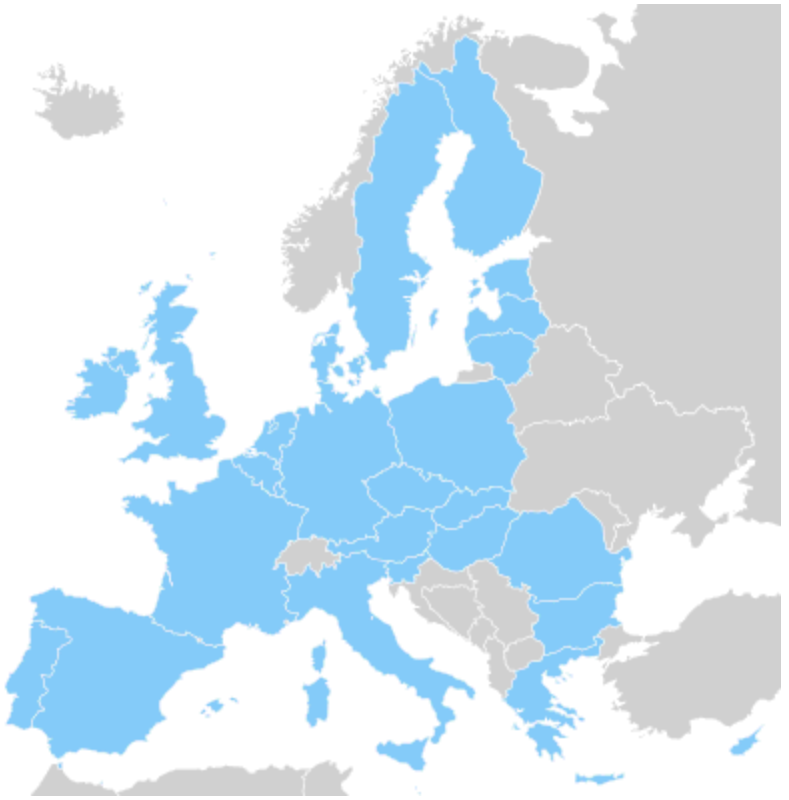


Understanding the European Union

an area of freedom, security and justice

- European Union (EU)
  - European Economic Area (EEA)
- Schengen
  - Police co-operation
  - Border Control
- Member States
  - Old Member States
  - New Member States
  - Candidate States
  - Applicant States
  - Potential Candidate States

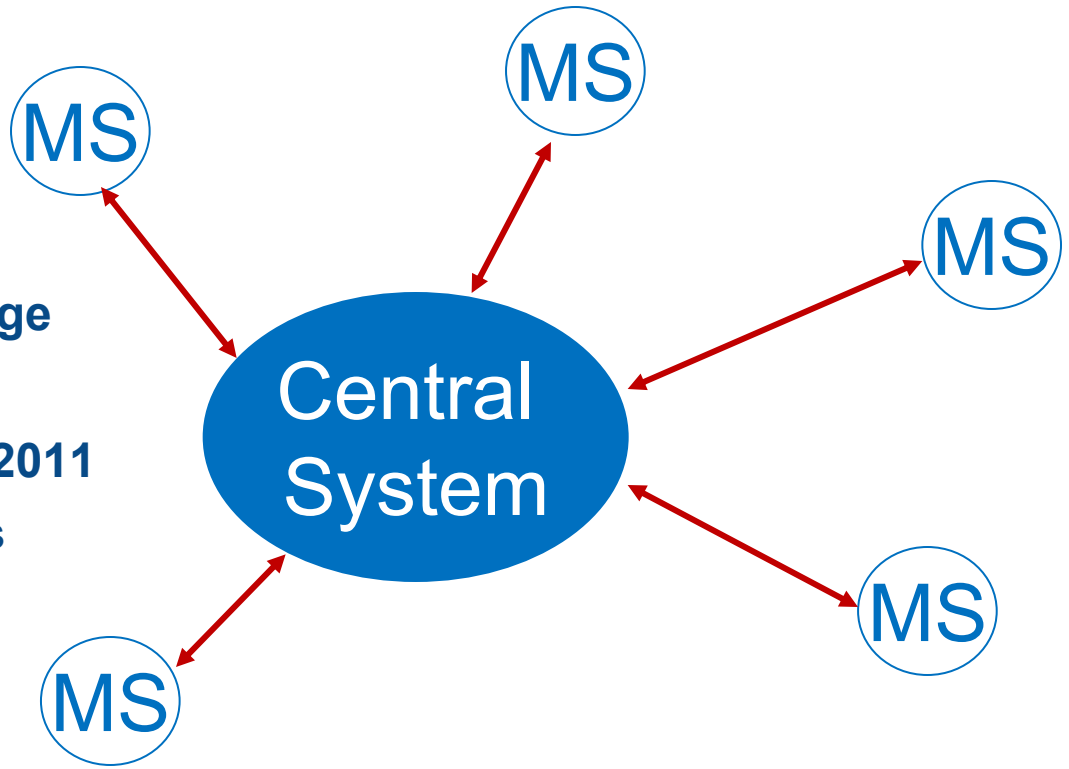
Enlargement



Data Sharing Models in the EU

Centralised

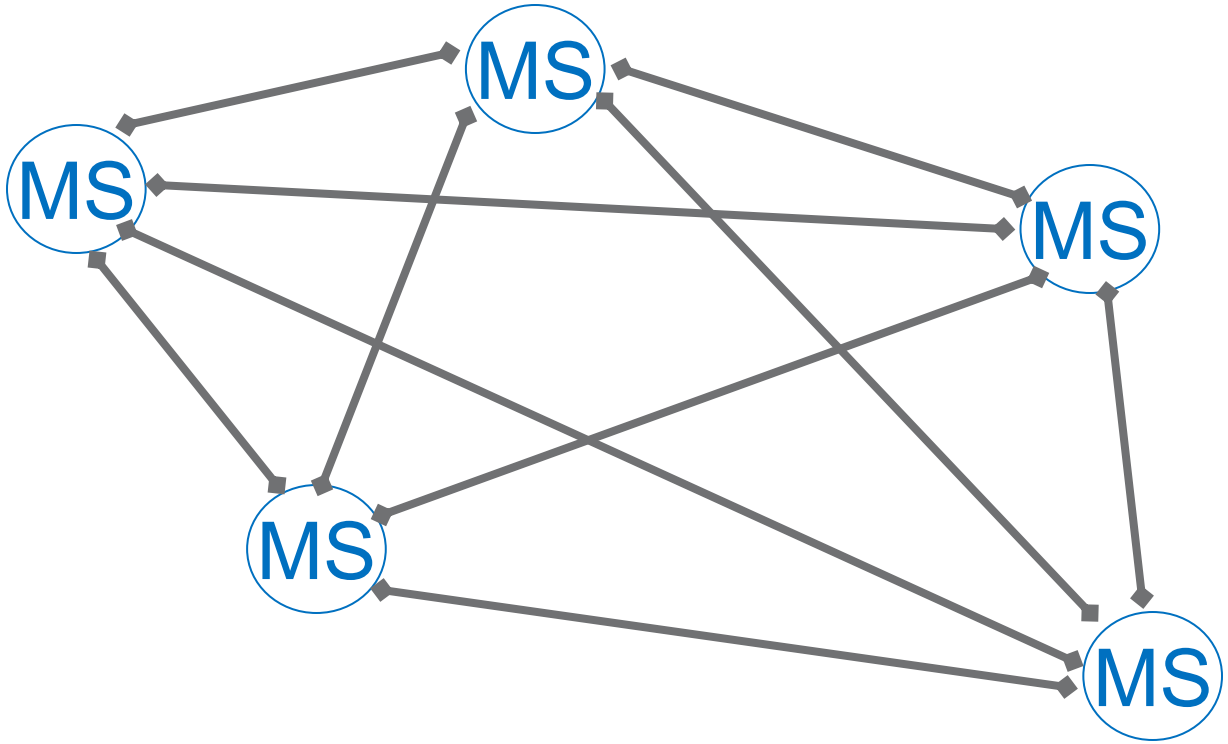
- **EURODAC (EU Asylum System)**
  - **Tenprint rolled**
  - **No alphanumeric data**
  - **Live since Jan 2003**
- **EU VIS (EU Visa System)**
  - ✓ Biometric Matching System
  - **Alphanumeric data + facial image**
    - ✓ 10 prints flat
  - **Operationally ready 24th June 2011**
    - ✓ Visa applications with biometrics
      - staged worldwide rollout
    - ✓ Biometric Border Verification
      - 3years after go live



Data Sharing Models in the EU

Decentralised

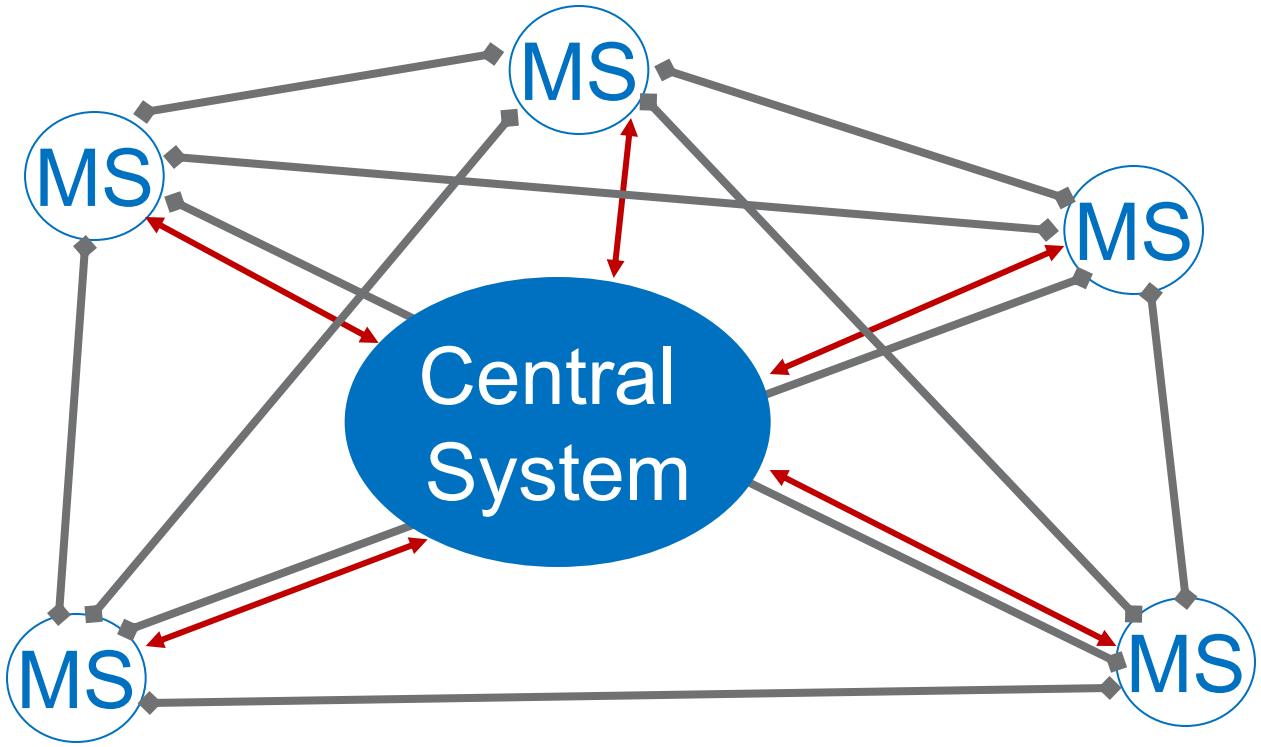
- **Prüm**
  - **Deadline Aug 2011**
  - **Fingerprints**
    - ✓ Tenprints
    - ✓ Palmprints
    - ✓ Latents
    - ✓ 7 MS live
  - **DNA**
    - ✓ 10 MS live
  - **Vehicle Registration**
    - ✓ 10 MS Live



Data Sharing Models in the EU

Distributed

- **Schengen Information System (SIS)**
  - **Alerts on people and goods**
  - **Biometrics exchanged via decentralised model**
  - **Live since 1995**
  - **SIS II**
    - ✓ Biometrics
    - ✓ Go live 2013 ?



SAFRAN Morpho

Under discussion

- **Exchange of Criminal Records**
  - **European Citizens**
    - ✓ Biometrics as an option
    - ✓ Decentralised model chosen
    - ✓ Due to go live April 2012
  - **Third Country Nationals**
    - ✓ Technical Study completed
    - ✓ Feasibility Study to be launched Spring 2011
      - Legislation changes
      - Data to be exchanged
        - » Many MS want it to be fingerprints
      - Model for the exchange
        - » Many MS pushing for centralised model

The Operational Challenges

Throughput

Decentralised Model

- **Incoming Transactions**
  - **Sizing**
  - **Storage**
  - **Memory**
  - **New workflows**
- **Outgoing Transactions**
  - **New Workflows**
    - ✓ Automatic or Manual Workflows
    - ✓ Additional Processes might mean additional Workstations
  - **Manual Verification**
- **Manage the transaction limits**

V

Centralised Model

- **Outgoing Transactions**
  - **New Workflows**
    - ✓ Automatic or Manual Workflows
    - ✓ Additional Processes might mean additional Workstations
  - **Manual Verification**

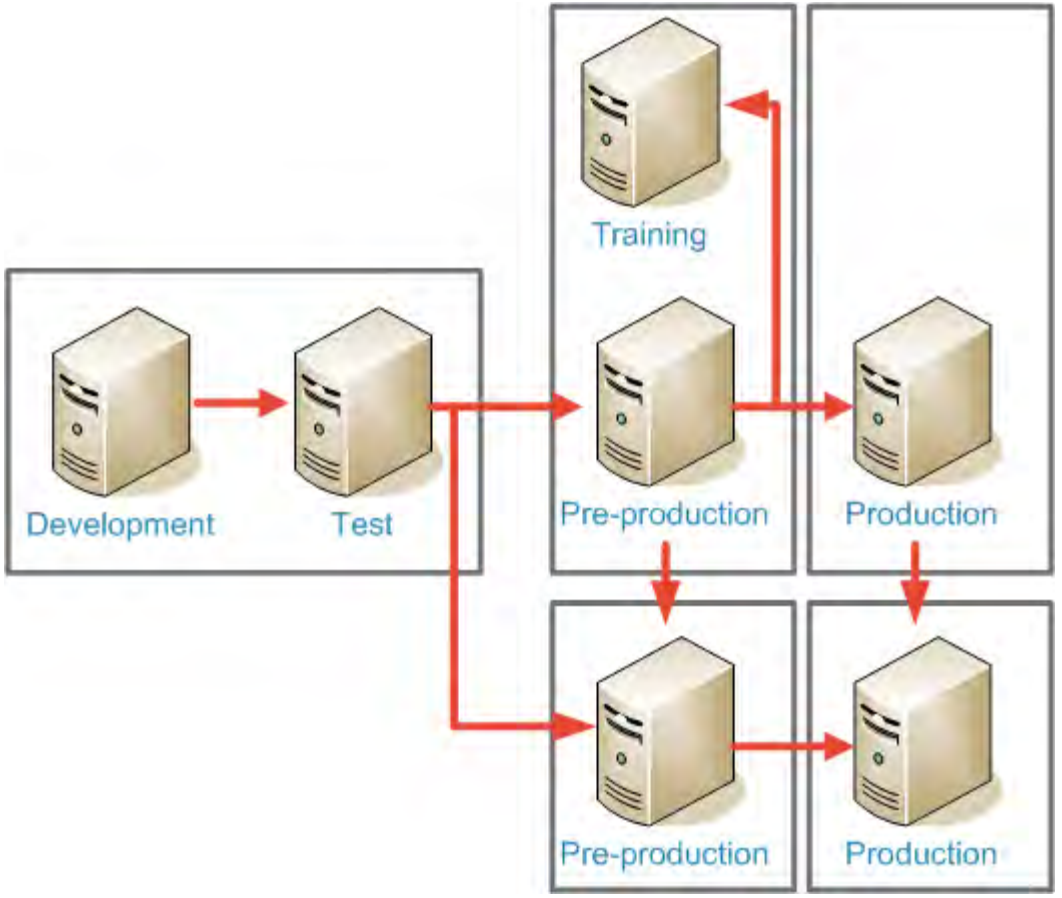
The Operational Challenges

Searching strategies

The Operational Challenges

Technical Infrastructure for decentralised model

- **Meeting the Response times**
  - **Higher resiliency**
  - **More IT domains to manage**
- **Testing**
  - **If 29 MS then**
    - ✓ with each MS = 28 tests
    - ✓ total no of communication tests = 812
  - **Can you test on an operational system?**
  - **Testing is not a one-off operation**
    - ✓ Will need this forever
- **Logging**
  - **Archiving of outbound and inbound responses might be required**
    - ✓ Prüm = 'all data'

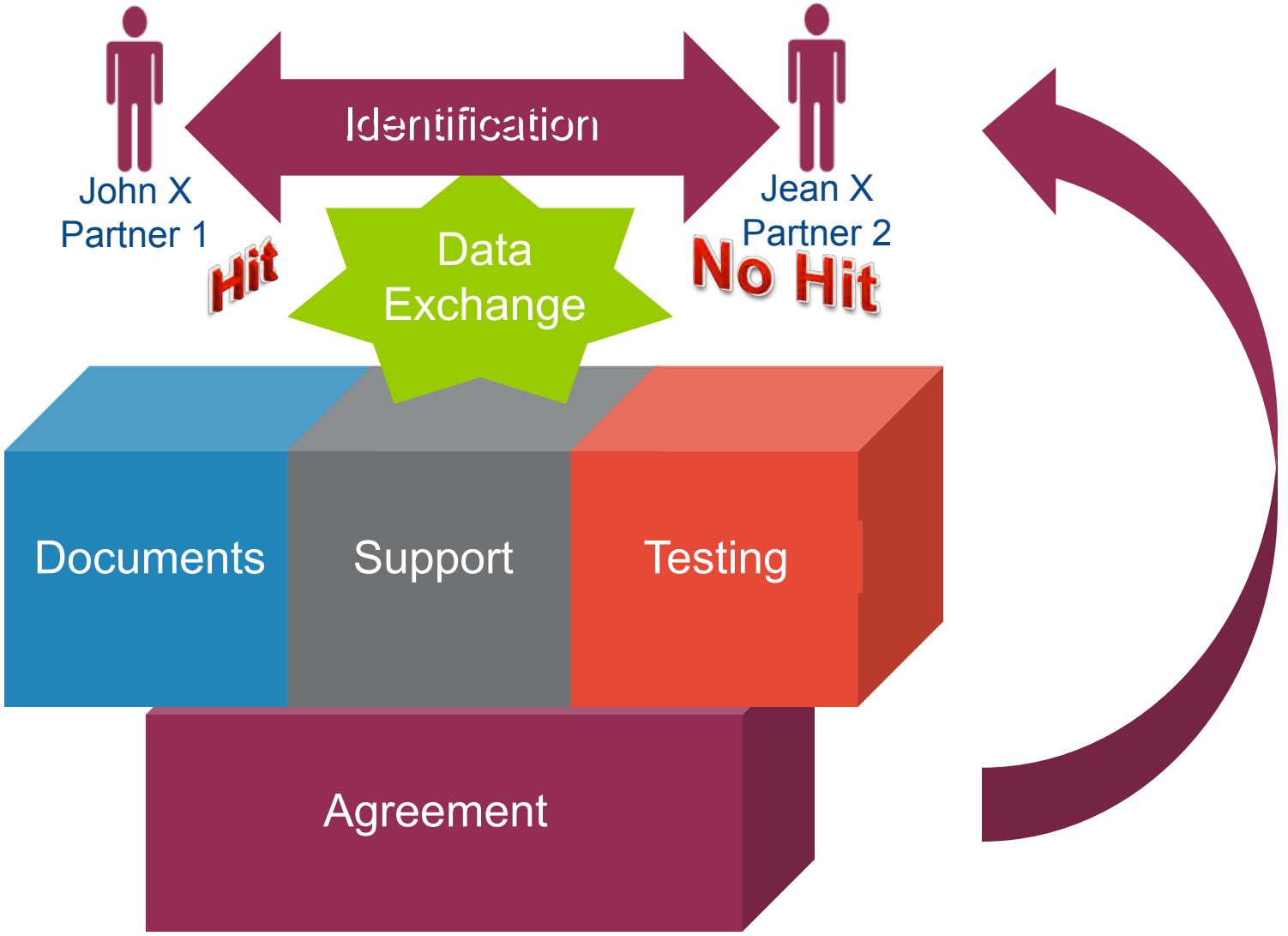


Building blocks for successful data exchanges

Success

Core data (biometrics)

Required Infrastructure



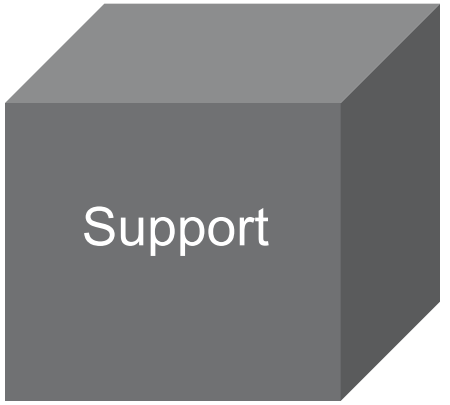
Building Blocks

Minimum requirements

- **Interface Control Document**
  - **Data to be exchanged**
  - **Types of Transactions**
    - ✓ Required for both core data and secondary data
- **Exchange Interface Document**
  - **Network definitions**
  - **Email addresses**
    - ✓ Need both formal and adminsitrative
  - **Certificate management**
- **Testing Document(s)**
  - **Communication tests between the network nodes**
    - ✓ Centralised : Once per partner
    - ✓ Decentralised : x*x-1
  - **Transaction Tests**
    - ✓ Test Data : need to be sure of the results of the tests
- **Final Acceptence / Go Live criteria**
  - What does it entail

Building Blocks

Resource Intensive



- Development of and understanding of FAQ
  - Pass on lessons learned
- Distribution of document updates
  - There are always errors in technical documents
  - Need a formal, fast way to disseminate information to all parties and their suppliers
- Management of Tests between partners
  - Central repository of test data
- Management and Distribution of certificates
  - If there are many partners, certificates will expire at different times
- Monitoring of Network
  - Most problems are network issues due to the number of stakeholders involved
- Training

Building Blocks

Resource Intensive

- **How is the testing organised**
  - **Communications and transactions tests can be performed separately**
  - **Time and resources**
    - ✓ Need dedicated personnel available to monitor results and resolve problems
- **How is testing performed on an operational system if no test system exists**
  - **Incoming transactions**
  - **Insertion of Test data**
  - **Logging**
    - ✓ If logs are used to create legal reports

Challenges

Organisational

- **After going live**
  - **What data should be submitted**
  - **Who decides what data should be submitted**
  - **Which Partner(s) should the data be submitted to**
    - ✓ The searching strategy
  - **Who verifies a hit from a request**
  - **Who supplies the alphanumeric data to a requesting partner who has verified a hit**
    - ✓ Might need dedicated ‘office’ to manage this
  - **Who deals with the issue when you exchange wrong data**

Funding

Who pays ?

Lessons learned

for success

- Standards are just the starting point
  - not the end of the road
- It is not just about adding software to handle automated exchanges
  - Biometrics work but success is actually based on the manual exchange secondary alphanumeric data not the first level core data exchange
- Organisational challenges are greater than the technical challenges
  - Data Sharing changes the back office processes for ever
- No matter what exchange model is chosen you need key building blocks for the model to work
  - Without them, everybody struggles and the real issues are misunderstood
- Funding
  - If procurements are controlled by each individual partner, timeframes for going live are long

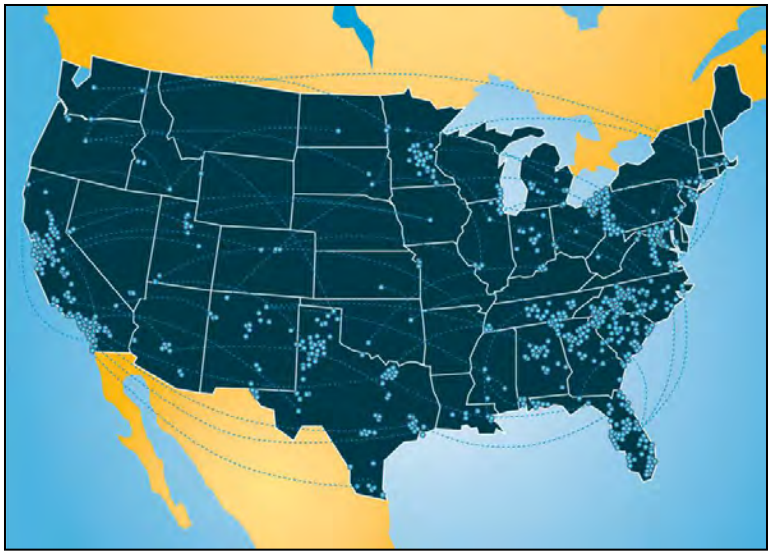
Thank you

Gillian Ormiston
Global Market Manager for Border Solutions
Email: gillian.ormiston@morpho.com
Tel: +44 773 880 8973

Using Biometrics for Retail Financial Services & Beyond

About AllTrust Networks

- Private, founded in 1999
- Pioneers in consumer-facing biometrics industry
- Successfully deployed biometrics to thousands of retail stores for identification & check cashing
- 6.5 million consumers enrolled to date

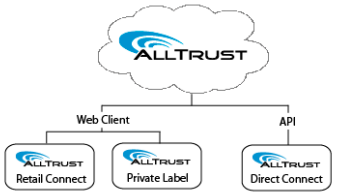


Intro to AllTrust

Our PC-based software minimizes the risks of cashing payroll and government checks. Like a credit bureau, we pool information and warn when transactions are risky.

AllTrust manages the largest opt-in commercial biometric database. We run a 'closed' network for good standing customers, and an 'open' network for known fraudsters.

We use high quality optical fingerprint scanners and technology from MorphoTrak. AllTrust has successfully secured PII data since product launch in 2000.



AllTrust's new Cloud platform provides a flexible web interface for biometric ID management and also integrates multiple financial services in addition to check cashing.

Alternative Financial Services Market

<u>38 million adults are either unbanked or underbanked</u>.* These consumers often get paid with a check on Friday evenings. Where do they go?

Banks

Grocery Stores
Convenience Stores

<u>Why?</u>

Won't give immediate cash
Limited hours
Don't trust banks
Negative history with banks
May lack US documentation

Immediate Cash
Extended hours
Clear Fees
Accept Alternate IDs
Fast & Friendly service

* 2009 FDIC sponsored study

AllTrust Adoption

Largest commercial biometric database for retail services

2,000+ active retail locations

6.5 million consumer enrollments with PII data

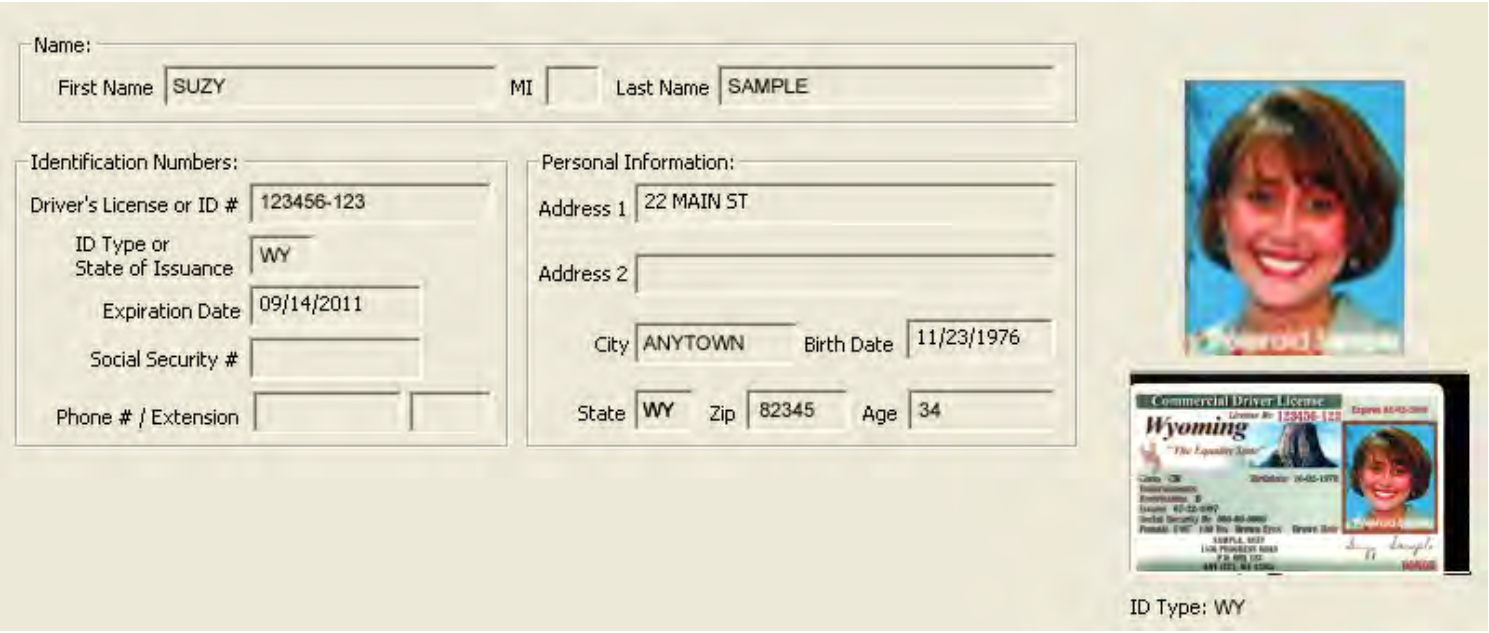
80 million check cashing transactions

$35 billion in check value processed

3.5 million check makers (issuers)

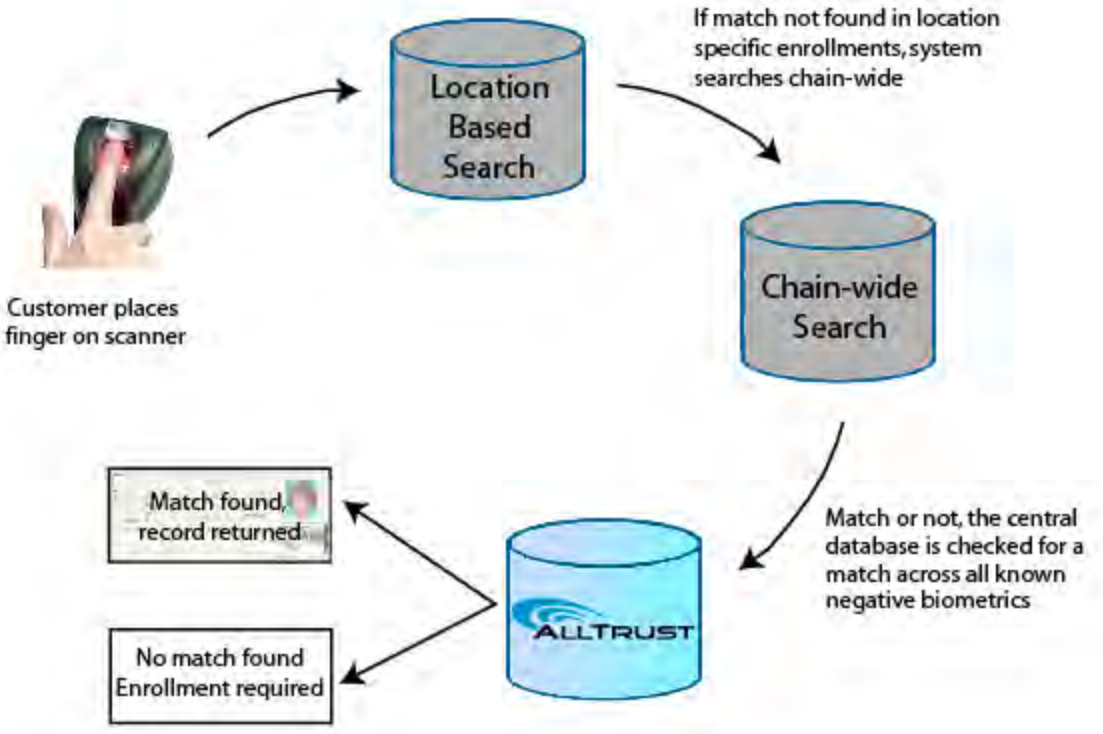
Enrollment & Securing PII Data

- Enrollment takes only 1 – 2 minutes
- Enrollment typically captures fingerprints (both index fingers), a picture of the individual, a copy of their driver's license or other ID, DOB, name and address (SSN and phone optional).



Identification / Verification Process

- Centralized database with real-time transaction processing
- Consumer simply places finger on the biometric sensor to identify themselves on return transactions
  - Record is retrieved in seconds
- Negative data is shared globally across the AllTrust network



Mitigating Fraud

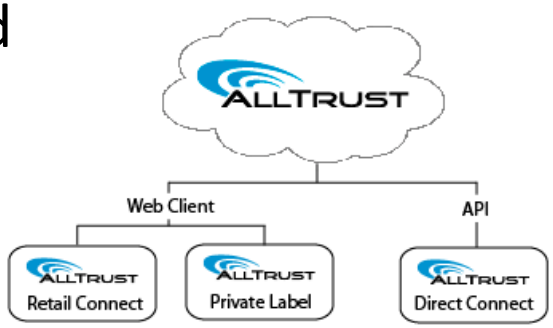
- Check fraud is a continuing problem for businesses today
  - 2009 ABA *Deposit Account Fraud Survey*:
    - Industry check-related losses amounted to ~$1.024 B in 2008
    - 80% of banks reported having check fraud losses
  - Information Security's Dec 2010 *Faces of Fraud Survey:*
    - Check fraud is one of the top three fraud forms plaguing banking institutions
- AllTrust minimizes fraud using a variety of tools
  - The biometric device discourages potential fraudsters and eliminates repeat offenders from using the system
  - The AllTrust network pools data and alerts retailers of risky transactions

Benefits for our Customers

- Improved Financial Performance
  - Cash more checks
  - Reduces write-offs
- Improved Customer Satisfaction
  - Faster Transactions
  - Reduces language barrier
  - Increased Security / No need to show ID or provide SSN
- Reduced Management Oversight
- Decreased Check Fraud Losses
  - Systematic rules mean fewer returned checks
  - Stops repeat offenders
- Biometric Benefit
  - Positive ID, ensures you know for whom you're performing a transaction

What's Next? AllTrust Cloud

- Biometric identification via the AllTrust Cloud
  - Identify or Verify individuals
  - Perform risk analysis
  - Leverage biometric ID for any application
  - Flexible and secure enrollment



- Open platform means that service is easy for partners to integrate and available on demand
- A suite of alternative financial services that can be customized for partners and retailers
  - Check cashing, money transfer, bill payment, telecom services, prepaid cards, etc.
  - Biometric ID will be leveraged for better customer service, BSA/AML Compliance and risk management

Summary

- AllTrust has demonstrated consumer and retailer acceptance of deploying biometrics for retail-based financial services
- Manages the largest commercial opt-in biometric database for retail financial services (6.5 million people)
- New open platform leverages identification and verification capabilities for any application using biometrics
- Looking for new opportunities & partners:
  - Government applications
  - Banking
  - Other

Thank You!

For more information contact:

Jon Dorsey

CEO

AllTrust Networks

(866) 324-6729 x510

Jon.dorsey@alltrustnetworks.com

www.alltrustnetworks.com

ACUITY
MARKET INTELLIGENCE

The Future of Biometrics
Mobility Rules

C.Maxine Most
Principal
Acuity Market Intelligence

NDIA
February 24, 2011
Arlington, VA

Today's Discussion

- Premise: Mobility Drives Biometrics
  - Mobility of Devices
  - Mobility of Individuals
- Critical Market Developments
  - Global Travel Identity Infrastructure
  - eCommerce and eGovernement
  - Convergence of Government and Commercial Platform
  - Mobility Drives the Enterprise
- Many Faces of ID Mobility
- Implications

About Acuity

Acuity consistently delivers thought-provoking, hype-free, data-driven insight and analysis

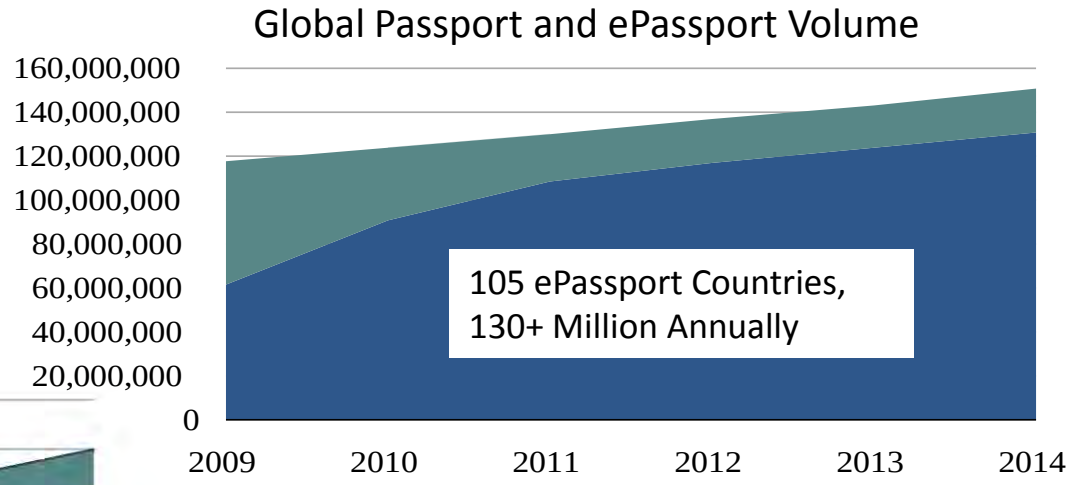
- Founded in 2001
- Proven accurate market analysis
- Led by industry experts C Maxine Most & Rudie Lion
- Singular focus on electronic people identification
- Latest research: Global and Regional ePassport and eVisa and National ID Industry Reports

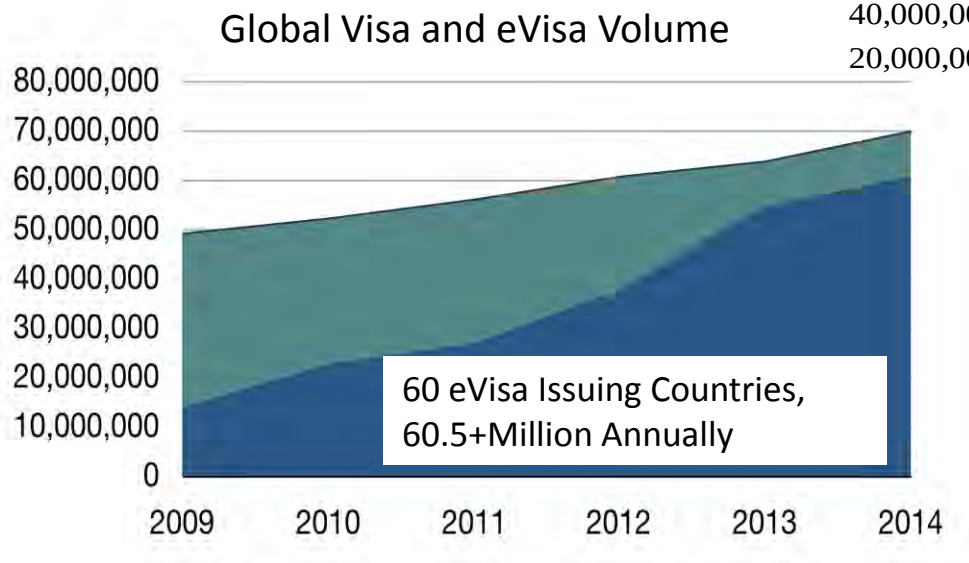
Premise: Mobility Drives Biometrics

Mobility and Associated Infrastructures, Platforms, and Applications are the Key to Understanding Biometric Market Evolution for the Forseeable Future

Global Travel Identity Infrastructure

By 2014, 87% of all Passports issued will be ePassports and 87% of all Visas issued will be eVisas





eCommerce & eGovernment

- 60 Countries with National eID Platforms
  - Many “Multi-Application” and Biometric
    - Government Services: Healthcare, Welfare, Travel Cards
    - Commercial Services: Banking, Transportation, Micro Payments
  - India’s UID conceived as Domestic Platform for host of Commerce and eGovernment Services
  - Germany’s NEW National ID re-visioned as a multi service card - meets both ICAO and EC travel card standards
- Very Successful NFC-enabled Mobile Payment Trials on EVERY Continent
  - Handset Manufacturers, Mobile Operators, and Financial Institutions are collaborating on NFC-enabled Transaction Infrastructure

Commercial Market

- The iPhone Changes EVERYTHING
  - Your Phone is your Life
  - "there's an app for that!”
- Devices are getting smarter, faster, more accessible AND cheaper
  - Sensors embedded in Device: pointer, on/off switch
  - NFC is coming full-throttle
  - Dual Facing Cameras
  - Payment Processing

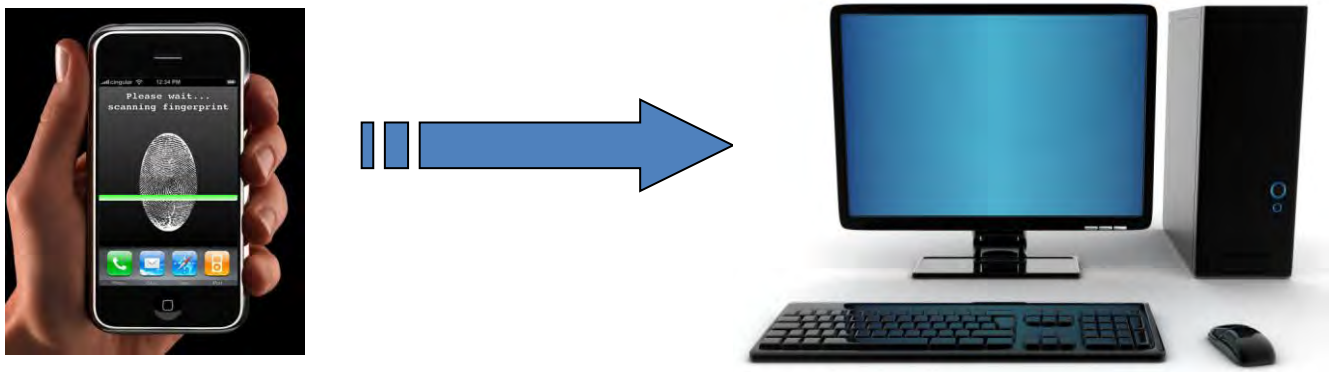
- And there are MORE OF THEM
  - 5B phones for 6.9B people = 72.6 %
  - Russia 147%, Italy 125%, Hong Kong 187%, Montenegro 192%
- Mobility in the field expands “Biometric” footprint
- RESULT: Mobilitiy will Drive Enterprise Adoption

Government Market

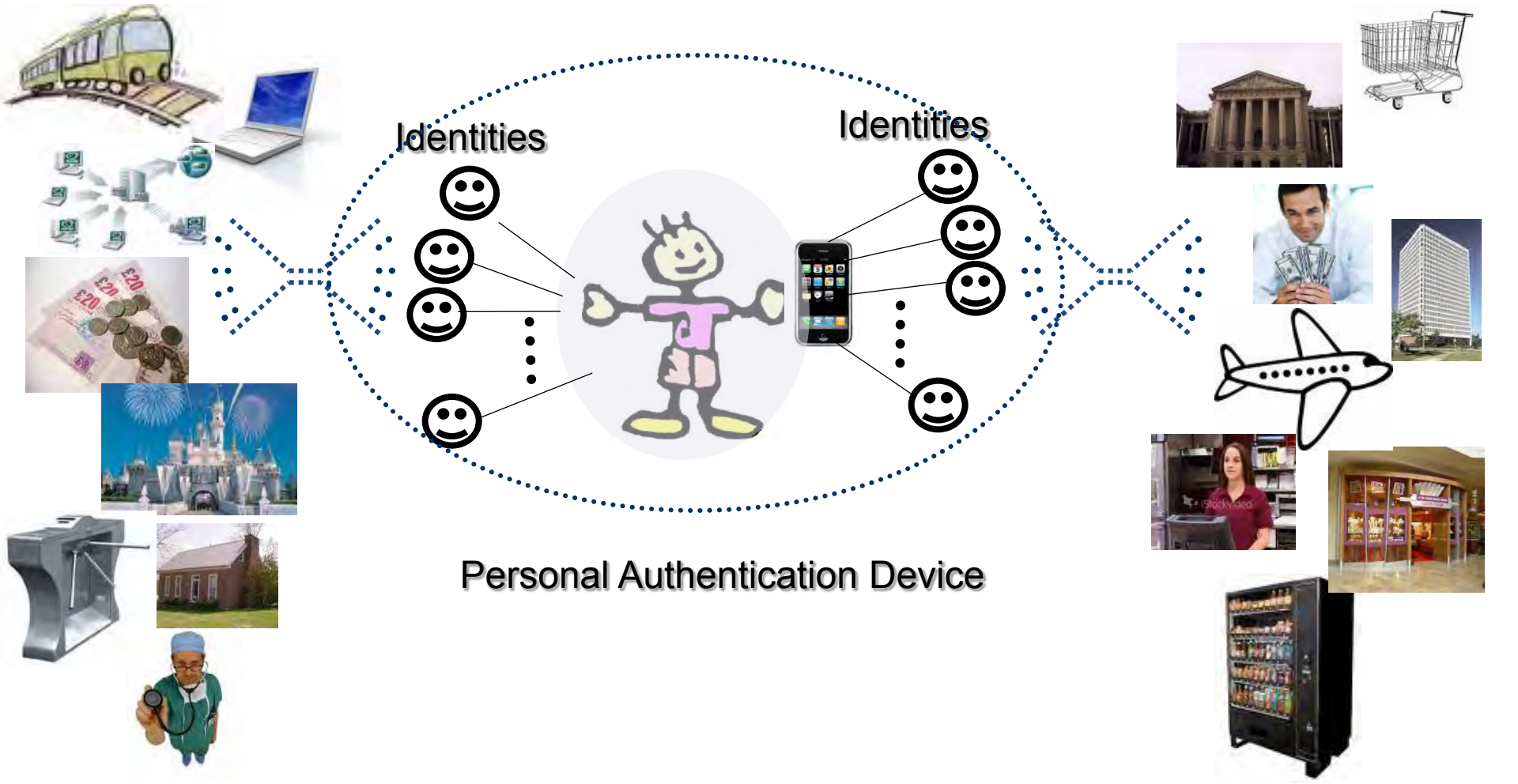
- iPhone's for All - ”is there an app for that too?”
- Multi-modal (e.g. multiple sensors/readers) Integrated Devices
- Very Successful for multiple scenarios
  - In the Field
  - In Theatre
  - At the Border
- Devices are getting smarter, faster, more versatile AND cheaper
- Field Based Government Services expand footprint
- Mobile Devices Drive Enterprise Level Adoption

Mobility Drives the Enterprise

- Once again, the iPhone Changes EVERYTHING
  - Proliferation of Mobile Devices an IT NIGTHMARE
  - ”Is there an app for that?”
- Devices are getting smarter, faster, more accessible AND cheaper
  - Everybody is using them all the time for CRITICAL proprietary, high-security Data and File Access and Communications
- Biometrics secure Mobility in the field; Better secure the Home Base as well



Many Faces of ID Mobility



Market Implications

- Mobility Creates a Bottom-Up Evolution
- Biometrics is Enabling Technology, SO Enable Something
  - Secure Platforms and Transactions
- Innovate and Standardize
- Build Commercial Solutions; Leverage Government Infrastructure then Customize for Government

ACUITY
MARKET INTELLIGENCE

Thank you !

For more information on or to preview Acuity's research and analysis

please visit www.acuity-mi.com

C. Maxine Most
+1 303 449 1897
cmaxmost@acuity-mi.com

Biometric Identification: It's Complicated

Melissa Ngo, Esq.
Privacy and Information Policy Consultant

National Defense Industrial Association

National Security through Biometric Collaboration:
A Roadmap to Tomorrow

February 23, 2011

Arlington, Va.

Definition and types

- Automated recognition of an individual based on physical or behavioral characteristics

- Includes scans of finger, iris, face, palm, voice, brain, DNA

Before you begin . . .

Some questions to ask:

- What is the purpose of the system to be created?
- What is the scope of the system?
- Is biometric ID likely to be the best system to reach your goal? Why?
- Do its benefits outweigh implementation, security, and other costs?
- How will you ensure security and privacy of the system?

Complex systems

- Biometric systems can include:
  - Physical parts: Database of biometrics, machinery to scan biometrics for input into database and to query database, people who enter or evaluate the biometric, outside auditors
  - Policy parts: Who has access and when? What if person can't or won't give the required biometric? What happens if there is a false match or false nonmatch? What happens if there is identity theft or fraud?

Problems with biometric-gathering

- Physical problems
- Religious or cultural problems
- Discomfort problems
- Failure to enroll problems could lead to discrimination or disenfranchisement

Privacy concerns

- Covert collection
- Unintended purposes (mission creep)
- Secondary information

Reliability questions

- Systems can be compromised
- Error rates in question
  - False matches/positives;
  - False nonmatches/negatives
- High-profile mistake: Brandon Mayfield case

Lowering privacy and security risks

- How is the system set up, protected, and maintained?
- Stringent security and audit trails
- Outside audits
- Allow people access to their records, remedies
- Limit retention, sharing and purposes

Louisiana TOTS

Tracking of Time Services

Creating a Win-Win through technology

Nicole M. Geller
Account Manager

ACS
A xerox Company

A bit about ACS

- Founded in 1988
- Fortune 500 Company and S&P 500
- $5.9 Billion (CY10) in Business Process Outsourcing (BPO)
- 78,000 Employees Worldwide
- Acquired by Xerox in February of 2010, now: ACS, a Xerox Company
- Providing services to more than 1,700 federal, state and local governments, making us the largest provider of BPO solutions to government in the U.S.
- Transportation projects in more than 30 countries
- Group Headquarters in Washington DC

Service Overview

- Subsidized care was historically paid based on provider declaration of attendance through a paper-intensive reporting and data entry system
  - Incorrect payments, fraud, and paper processing overwhelmed both providers and states

- ACS e-Childcare tracks and calculates payment to subsidized child care providers based on actual attendance
  - Oklahoma and Indiana implemented in 2003 using POS terminals at provider locations (More recently: Texas and Colorado)
  - Parents were issued a magnetic stripe card to check children in and out of care through a POS terminal, creating a record of actual attendance

TOTS Requirements

- Louisiana loved the system but wanted to utilize finger imaging rather than cards as the identification medium for parents
  - ACS partnered with MorphoTrak to design and develop the biometric identification methodology

- Parents/authorized representatives record finger image at local parish offices
  - Images are captured and stored on the ACS EPPIC system
  - Images are downloaded to appropriate provider POS devices nightly

- Parents scan finger at check in/check out on readers attached to POS devices at child care centers

041.LA

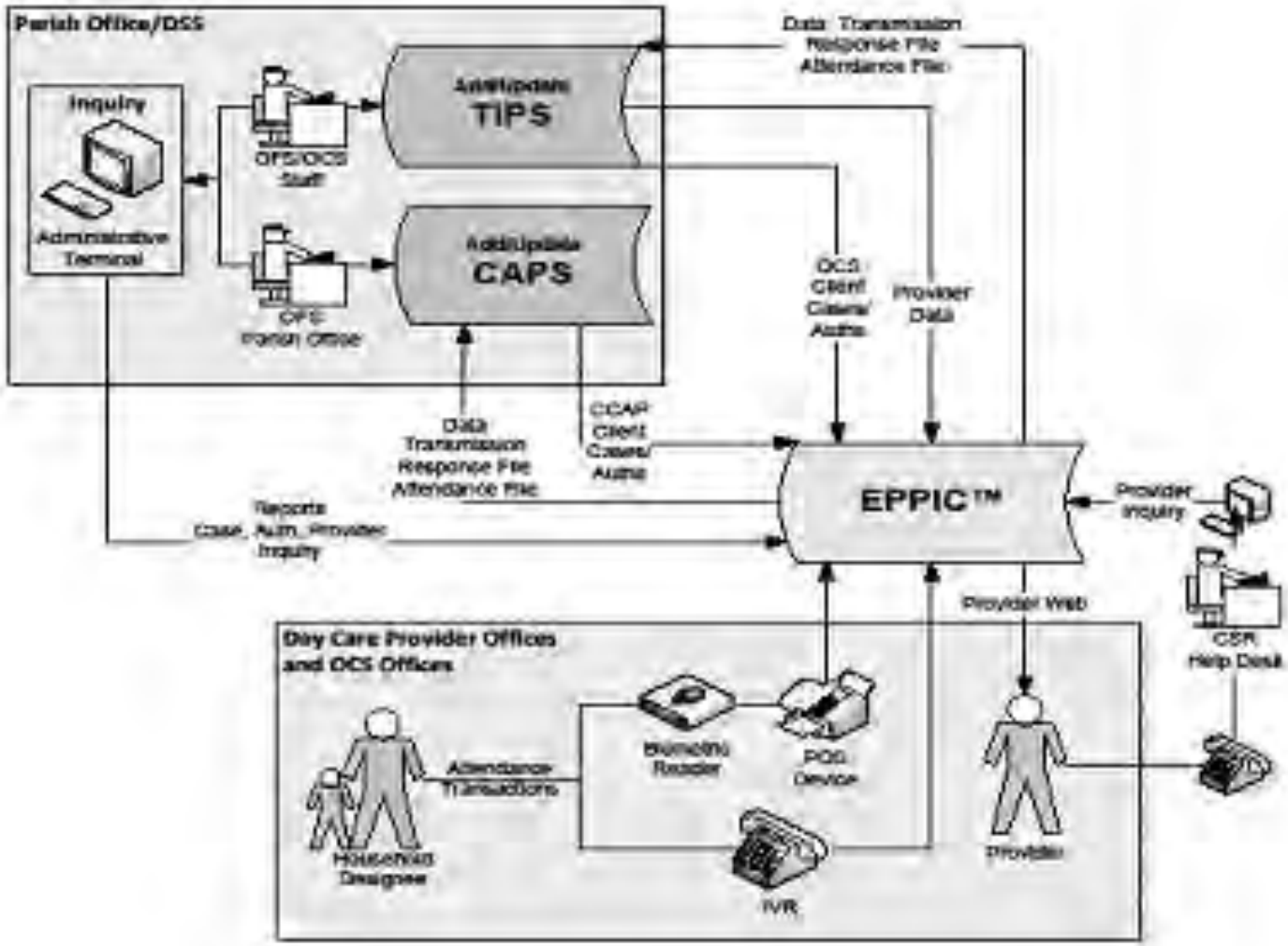
042.LACCT

ACS
A xerox Company

TOTS Requirements

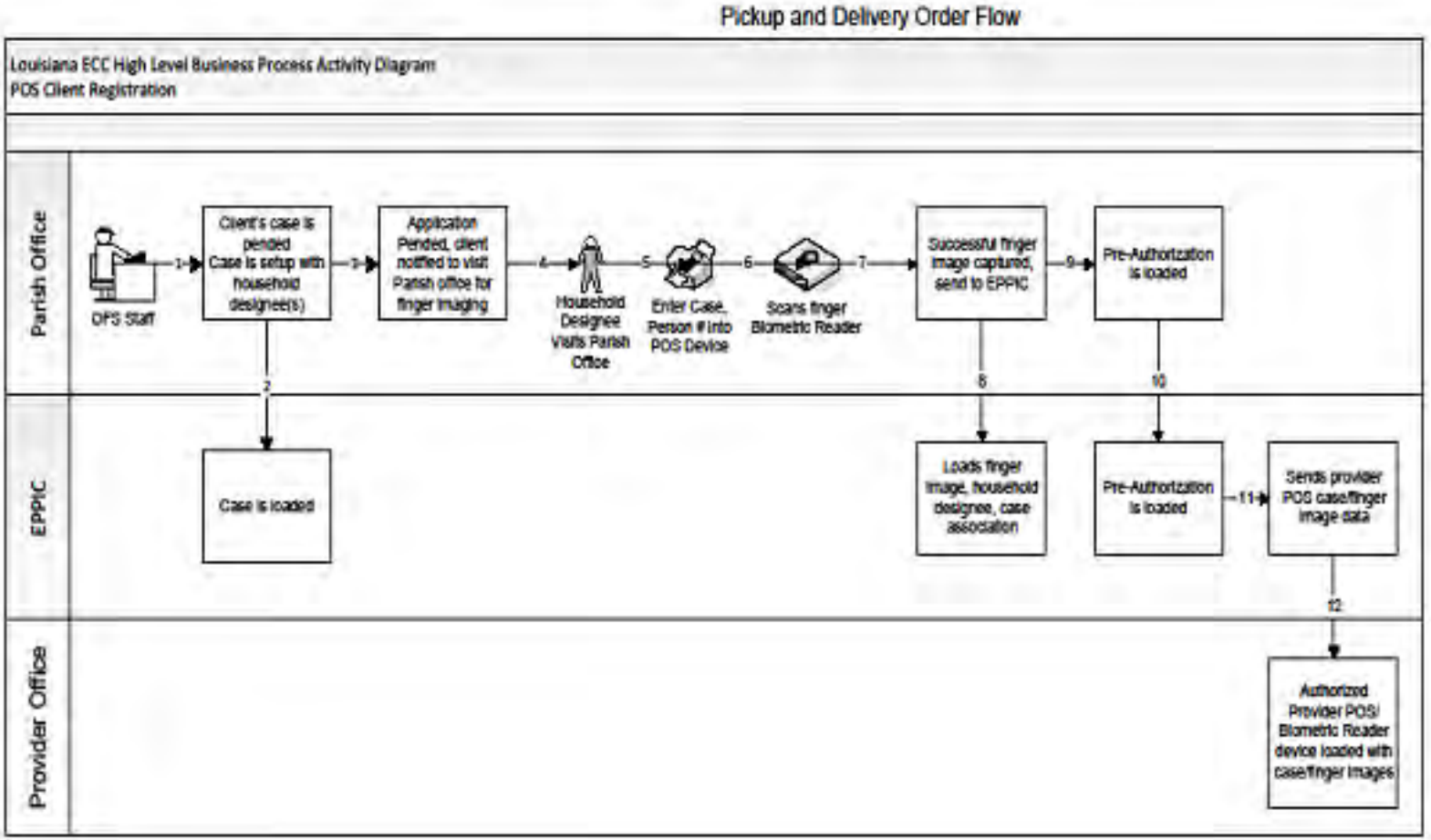
- Comprehensive service
  - Interface capability with State systems
  - Capture and record attendance transactions
  - Training
    - State staff
    - Providers
    - Clients
  - Payment calculation
  - Extensive reporting including real time updates of attendance

TOTS Business Flows – System Interfaces

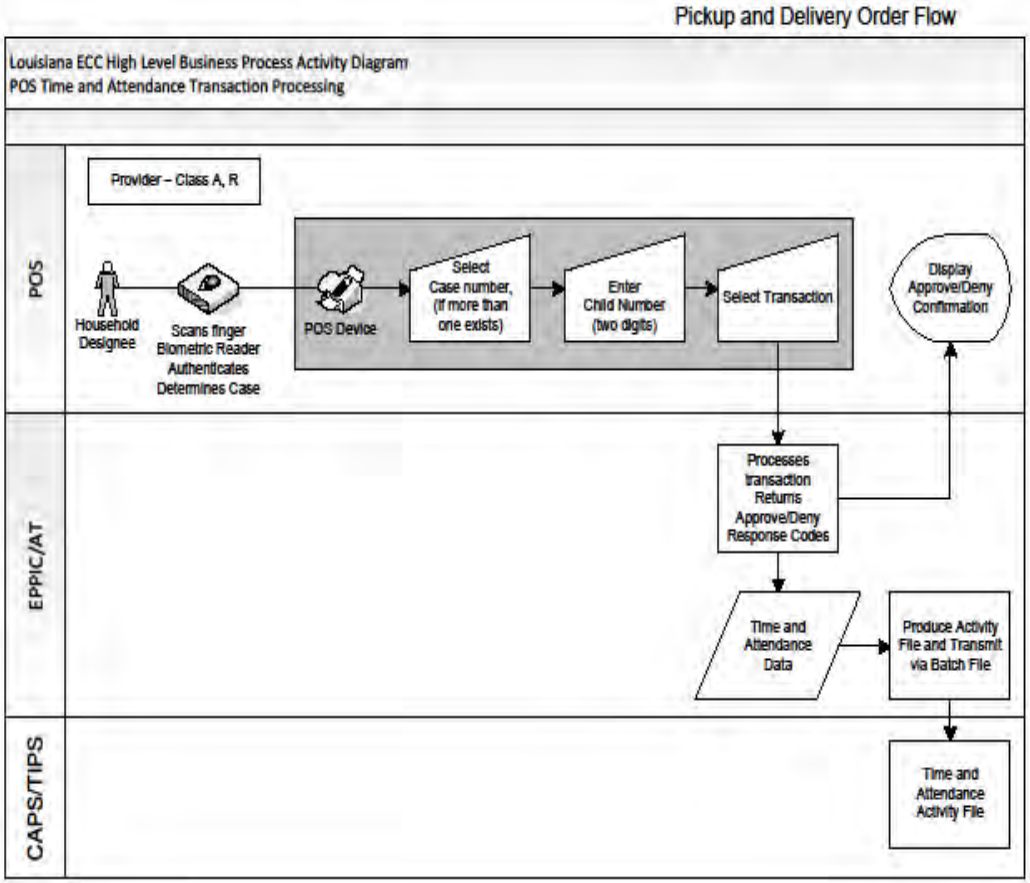


ACS
A xerox Company

TOTS Business Flows – Client Registration



TOTS Business Flows – Attendance Transaction Processing



TOTS Success – Win/Win

- State savings still being calculated but appear to be beyond expectations
  - Allows the State to serve more children and eliminate fraud
  - Automation allows the State to achieve administrative savings through elimination of data entry of payment forms, elimination of printing, mailing, and reissuance of lost checks
  - Data and reporting available through the TOTS system allows federal, state, and legislative reporting to be generated on line
- Providers eliminate labor intensive attendance form completion and receive regular, timely payment for actual attendance
- Provider portal allows providers to instantly access on line attendance and payment data
- Clients are in control of attendance and payment to providers
- Swipe of finger image inherently provides parent attestation that care was rendered

Benefits of biometric technology in eChildcare

- Single benefit child care cards can be given to child care providers – fingers cannot
- Requires parents to visit child care provider regularly – important to state programs who want to encourage parent involvement in care of their children
- Has demonstrated the benefits of the technology in social service environments
- An individual's finger image association to a case provides additional Provider controls over who is and is not authorized to pick up a child

Biometria.AR

"National Network of Biometric Information"

Jefatura de
Gabinete de Ministros
Presidencia de la Nación

What about the ONTI ?

(National Office of Information Technologies)

Mission

- ✓ Open Government , Digital Agenda & e-Government
- ✓ Computer Emergency Response Team (ArCert)
- ✓ Critical Information Infrastructure Protection
- ✓ Technological Standards for the National Administration

✓ Biometrical Latinamerica

Overview

Leading Cases in the Field

✓ Biometrical Argentina

Overview

Biometria.ar Project

COUNTRY	≈ SIZE
MEXICO	111,3
VENEZUELA	63,1
BRASIL	55,4
ARGENTINA	35,9
CHILE	15,8
GUATEMALA	15,1
EL SALVADOR	7,9
HONDURAS	7,5
COSTA RICA	6,6
URUGUAY	5,4
PANAMA	4,7
BOLIVIA	4,1
REP DOMINICANA	3,0
ECUADOR	2,7
JAMAICA	2,6
BAHAMAS	N/R
BARBADOS	N/R
PARAGUAY	N/R
PUERTO RICO	N/R
TRINIDAD Y TOBAGO	N/R

LATINAMERICA

(from Mexico to Argentina)

Countries Studied:

19

Biometrics Records available:

291.5 million

Projects in current development or to be developed:

78

FUENTE: Estudios Propios (relevamientos propios en base a noticias de adquisiciones y proyectos en fuentes por prensa y difusión)

LATINAMERICA

COUNTRY	≈ SIZE M	POPULATION M	RATIO %
MEXICO	111,3	108	103
VENEZUELA	63,1	29	217.5
BRASIL	55,4	191	29
ARGENTINA	35,9	40.1	89.5

Highlights::

A single individual recorded in different databases for different uses/objectives

There is no master biometric record for every transaction

Many biometric systems holding different options for enrollment and search

Multiple suppliers systems

No interAFIS/interABIS systems within the same country

FUENTE: Estudios Propios (relevamientos propios en base a noticias de adquisiciones y proyectos en fuentes por prensa y difusión)

ARGENTINA

Population: 40.1 million
Inhabitant/Registry Ratio: 89.5%
Government: FEDERAL – 23 provinces and 1 autonomous city

LAW 17.6.71 : «*Art.7 - … assigning every individual an identification record, with an exclusive and unalterable ID number (…) There will be, at least, patronymic, numeric and dactyl files, according to the Argentinean Vucetich system or any other in line with future developments…*»

ID Documents:

- National ID (DNI): Booklet for Voting and portable ID-Card
- Argentinean Passport

ARGENTINA

Borderline:

- ✓ **Chile:** **5.526 km** with **80** control stands
- ✓ **Brasil:** **1.132 km** with **14** control stands
- ✓ **Paraguay:** **1.737 km** with **9** control stands
- ✓ **Bolivia:** **752 km** with **5** control stands
- ✓ **Uruguay:** **493 km** with 3 control stands

Land Borderline: 9.370 km (3 x USA-MEXICO)

Federal	FEDERAL ARGENTINEAN POLICE (PFA)	15 million forensic ABIS records (2010)	SAFRAN-MORPHO
	FEDERAL PENITENTIARY SERVICE (SPF)	50 thousand ABIS records (2010)	GOLDENFINGER
	NATIONAL RECIDIVISM REGISTRY (RNR)	3 millions (update to 5 M) AFIS records (2010)	NEUROTECHNOLOGIJA
	NATIONAL IMMIGRATION DEPARTMENT (DNM)	500 thousand ABIS records (PILOT-2010)	NEC
	CITIZEN NATIONAL REGISTRY (RENAPER)	Capacity to 15 million civil records	NEC
states	BUENOS AIRES	3 million forensic ABIS records	SAFRAN-MORPHO
	CORDOBA	250 thousand forensic ABIS records	SAFRAN-MORPHO
	CHUBUT	100 thousand forensic AFIS records	SAFRAN-MORPHO
	LA PAMPA	90 thousand forensic AFIS records	SAFRAN-MORPHO
	NEUQUEN	100 thousand forensic AFIS records	SAFRAN-MORPHO
	MENDOZA	100 thousand forensic AFIS records	COGENT SYSTEMS

Actualizado a 2011 – febrero – Fuete: observatorio www.biometria.gov.ar

FEDERAL AGENCIES – CURRENT SITUATION

	INSTITUTION	DACTYL	FACIAL	IRIS	VOICE	SIG	OTHER (ADN/SMT)	PATRONYMIC
1	**General Citizen Register Office** RENAPER	☑						☑
2	**Federal Argentinean Police** PFA	☑	☑		☑	☑	☑	☑
3	**National Gendarmerie** GNA	☑	☑		☑			☑
4	**National Coast Guard** PNA	☑						☑
5	**Airport Security Police** PSA		☑					☑
6	**National Immigration Department** DNM	☑	☑					☑
7	**Federal Penitentiary Service** SPF	☑	☑				☑	☑
8	**National Recidivism Registry** RNR	☑						☑
9	**Federal Public Revenue Administration** AFIP	☑						☑
10	**National Social Security Administration** ANSES	☑						☑

CURRENT ISSUES
AND CRITICAL POINTS

- No communication among systems
- Possible duplication of biometrical records with multiple patronymic information
- No National standard for biometric interoperability
- No National standard for biometric equipment
- Most of national agencies have not yet digitized all biometric records to data formats suitable for automated applications
- Information backup is on tapes or paper with no Business Continuity Center
- No biometric centralized records to check for any “no name”
- COST: US Dollar prices do not reflect the true procurement capabilities in Argentina

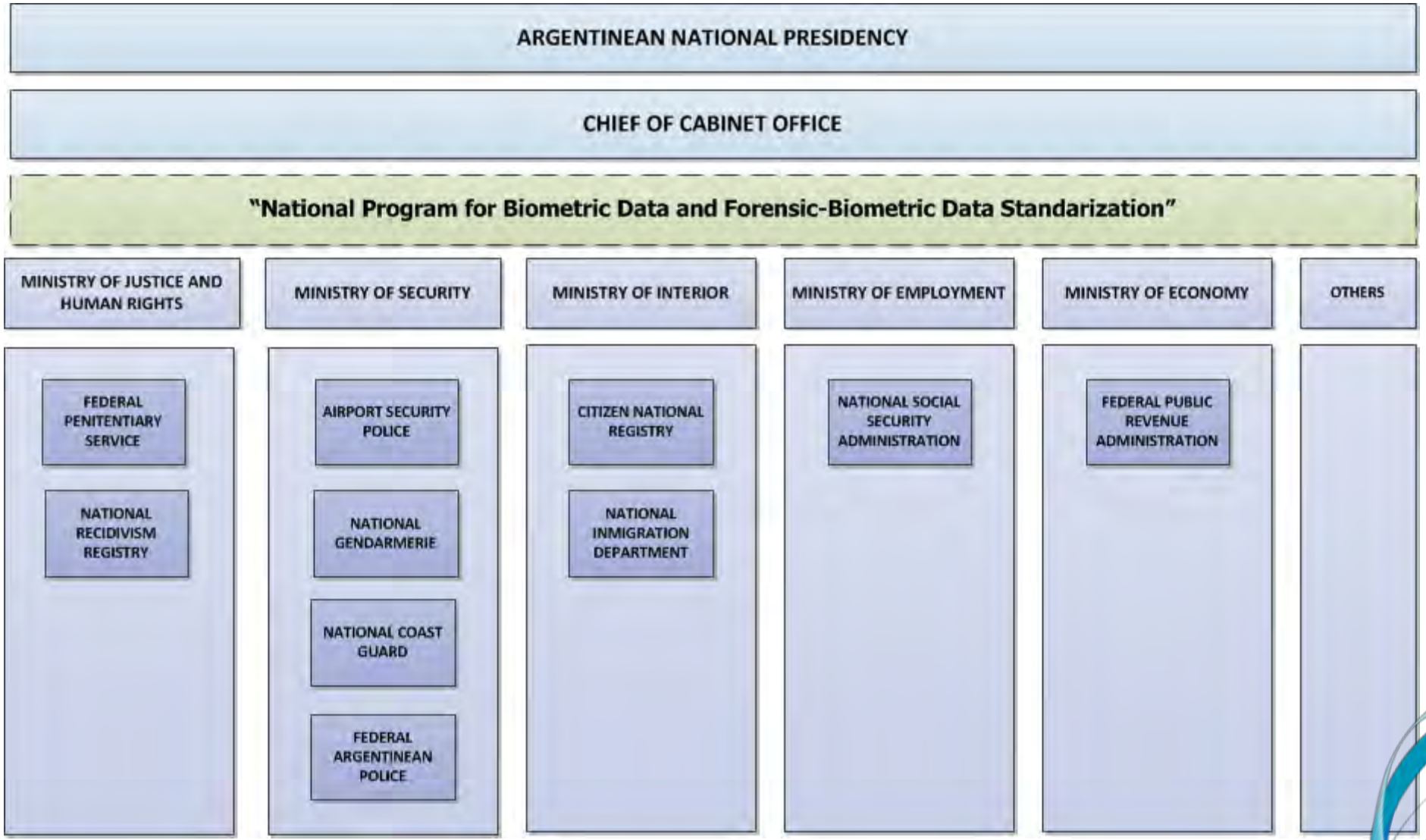
BIOMETRIA.AR

National Program for Biometric Data and Forensic-Biometric Data Standarization

TODAY we are working on…

PROJECT «BIOMETRIA.AR»

SCOPE



CURRENT PROJECTS
AND ONGOING ACTIVITIES

- To adopt and standardize XML interfaces for the biometric data interoperability

- To incorporate the FBI certification in the biometric hardware requirements for printing, digitization and live capturing in the Standards for the Federal Administration.

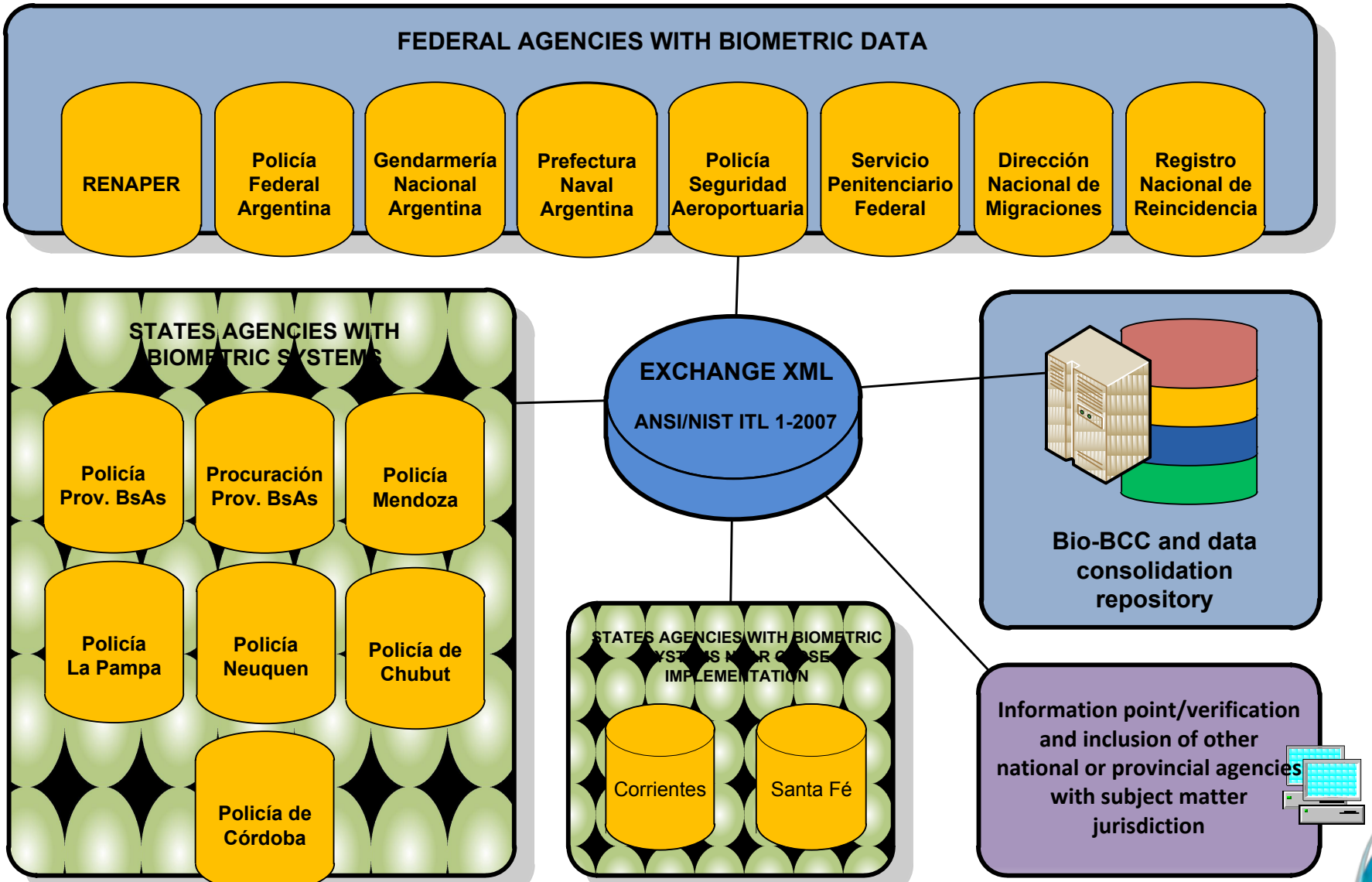
- To adopt and propose the implementation of a PIV (Personal Identity Verification) within the Federal Administration

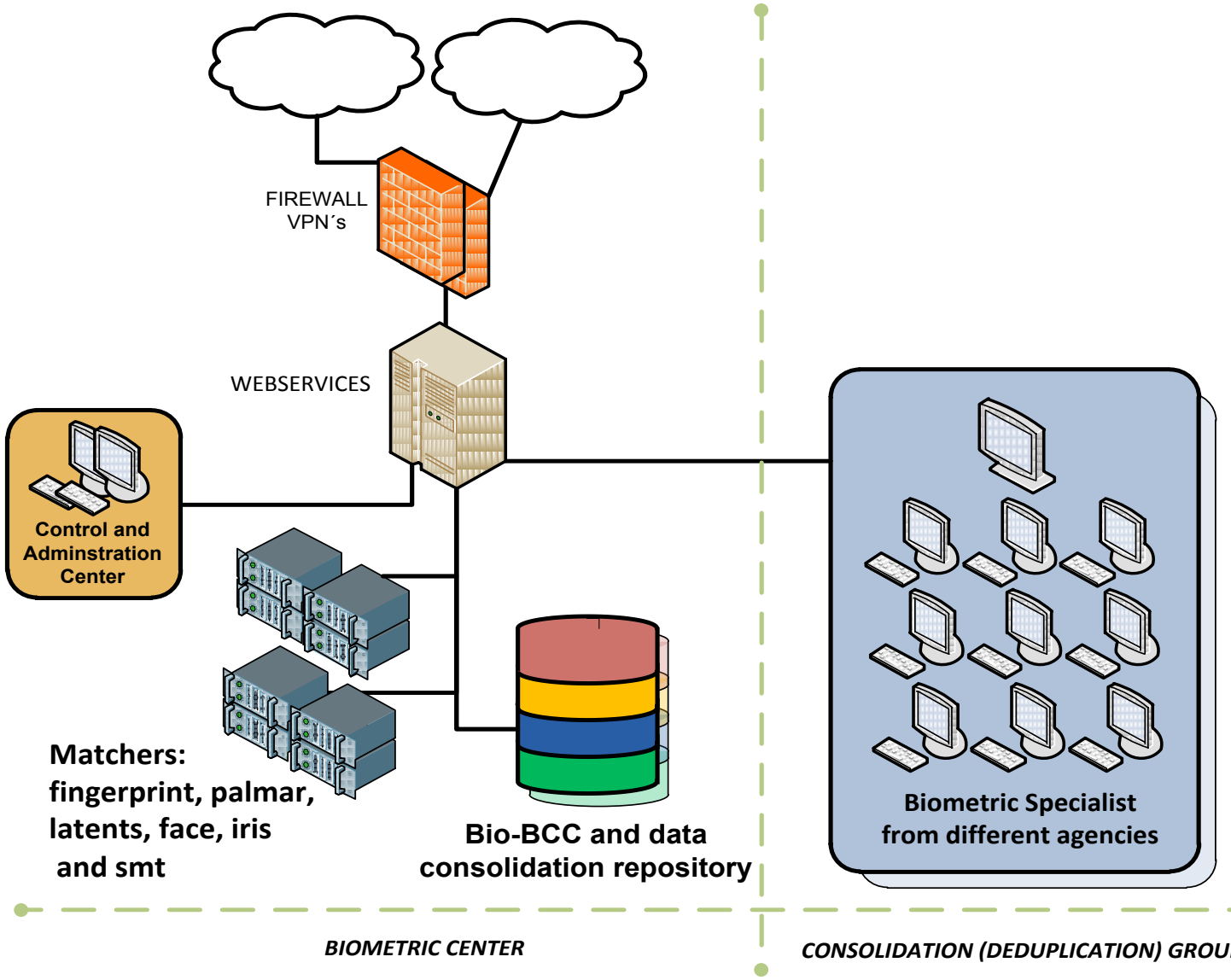
- To develop a centralized biometric registry of dead NN s (no names), NN s found and missing

- To implement a Business Continuity Center to save critical biometric data.

- To develop and encourage compliance of the best practices guide for the digitization of biometric forms

- Consolidating a single biometric identity


FEDERAL AGENCIES WITH BIOMETRIC DATA
RENAPER
Policía Federal Argentina
Gendarmería Nacional Argentina
Prefectura Naval Argentina
Policía Seguridad Aeroportuaria
Servicio Penitenciario Federal
Dirección Nacional de Migraciones
Registro Nacional de Reincidencia
STATES AGENCIES WITH BIOMETRIC SYSTEMS
Policía Prov. BsAs
Procuración Prov. BsAs
Policía Mendoza
Policía La Pampa
Policía Neuquen
Policía de Chubut
Policía de Córdoba
EXCHANGE XML
ANSI/NIST ITL 1-2007
Bio-BCC and data consolidation repository
STATES AGENCIES WITH BIOMETRIC SYSTEMS NEAR CLOSE IMPLEMENTATION
Corrientes
Santa Fé
Information point/verification and inclusion of other national or provincial agencies with subject matter jurisdiction


FIREWALL
VPN´s
WEBSERVICES
Control and Adminstration Center
Matchers: fingerprint, palmar, latents, face, iris and smt
Bio-BCC and data consolidation repository
Biometric Specialist from different agencies
BIOMETRIC CENTER
CONSOLIDATION (DEDUPLICATION) GROUP

FIRST STEPS TAKEN

In order to start with these actions the project for patronymic and biometric consultation was launched.

The first four national institutions selected are:

- **Federal Argentinean Police**
- **National Recidivism Registry**
- **National Immigration Department**
- **Citizen National Registry**

www.biometria.gov.ar

5th CIBRA

Jefatura de
Gabinete de Ministros
Presidencia de la Nación

Thank you

Pedro Janices

National Director | National CIO | **ONTI**

National Office of Information Technologies

pjanices@sgp.gov.ar

NIST Tests Supporting Biometric Identification Applications

Patrick Grother

Information Technology Laboratory
National Institute of Standards and Technology (US),
United States Department of Commerce

National Defense Industry Association's
National Security Through Biometric Collaboration: A Roadmap To Tomorrow
Sheraton National, Arlington VA, February 23-24, 2011

NIST

Overview

- Chapter 1. Biometric versatility
- Chapter 2. NIST Role
- Example NIST outputs
  - Chapter 3. Face Recognition
  - Chapter 4. Iris Recognition

NIST

Chapter I :: Uses of Biometrics

Biometric Versatility

NIST

Tactical Biometrics :: Versatility

1:1 Authentication :: Is he who he claims to be?

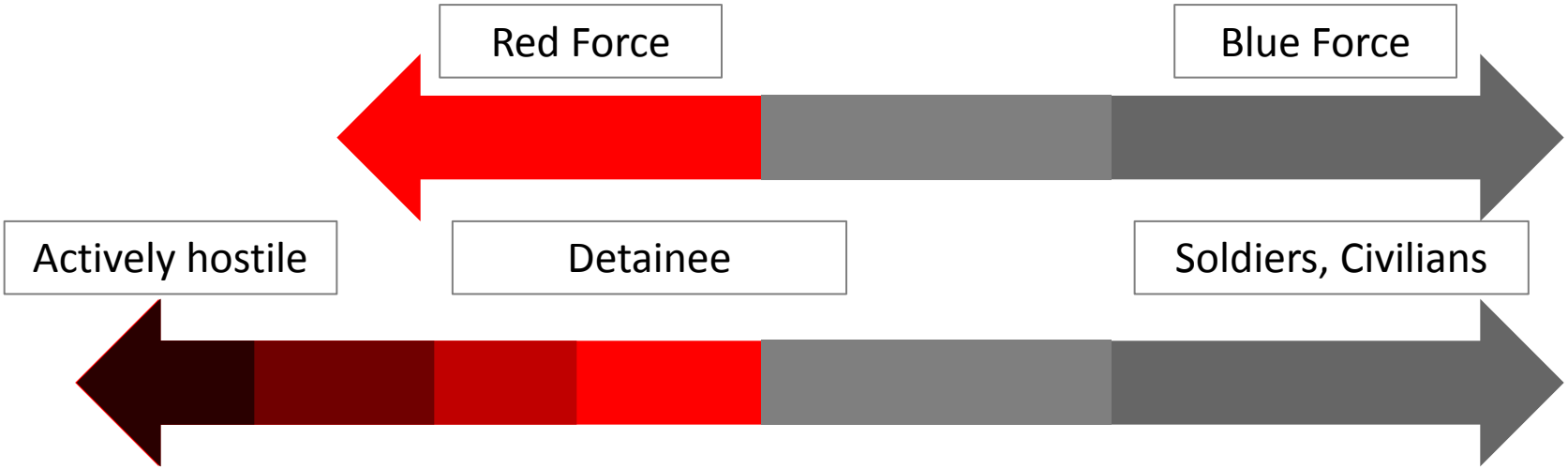
- Credential issuance
  - Bind ID to person who has been submitted to background check
- Access control
  - Physical access
  - Logical access

1:N Identification :: Who is she?

- Unique ID
  - Binding unique IDs and biometrics
- Duplicate detection
  - Identity fraud, visa, driving license
- Background check
  - Against criminal db, for example
- Watchlist - lookout
  - Surveillance
- Role-based access control
  - Token-less authentication
- Forensic applications
  - Latent collection
  - Crime scene video

NIST

Foe, Friend and Everything In Between and Beyond :: The Role of Biometrics



Un-cooperative	Non-cooperative	Cooperative
Difficult biometrics	Maybe covert biometrics	More overt biometrics
Opportunistic		Strategic Identity Dominance
Not Necessarily Persistent		Persistent
Standoff		Close range
Future		Current commercial capability

NIST

Chapter II :: NIST Activities in Biometrics

NIST

About NIST

- National Institute of Standards + Technology
  - Part of Department of Commerce
  - Non-regulatory
  - Non-policy
  - Charter, since 1901, is to support US Industry via
    - Measurement, Standards, Calibration, SRMs, SRDs
  - Bias toward transparency, publication
  - Write specifications for government IT systems
    - Federal Information Processing Standards (FIPS) are legally binding under FISMA legislation.

NIST

About Biometrics at NIST

- Information Technology Laboratory
  - Security Division, ~ 2 FTE
  - Information Access Division, ~ 24 FTE
- Biometrics
  - Fingerprint, Latent, Iris, Face, Speaker, DNA
  - Testing – performance , usability, reliability, interoperability
  - Testing standards – for technology, operational, scenario
  - Data interchange Standards – for interoperable law enforcement, for credentials, for networks
  - Research – Performance evaluation, Metrology, Security, Forensics, Image Quality, Multimodal fusion, Multi-sample fusion, Scalability, Face Recognition, Iris recognition,

NIST

NIST Programs Supporting Applied Biometrics

Standards

- Face Recognition
  - ANSI/NIST Type 10
  - ISO/IEC 19794-5
- Iris Recognition
  - ANSI/NIST Type 17
  - ISO/IEC 19794-6
- Fingerprint minutiae
  - INCITS 378
  - ISO/IEC 19794-2, A/N Type 9
- Speaker
  - ANSI/NIST Type X (Future)
  - ISO/IEC 19794-13
- Latent fingerprint
  - ANSI/NIST Type 9 EFS
- Fingerprint
  - ANSI/NIST Type 14

Testing

- FRVT / MBE / FERET
  - 1:1, 1:N Face Recognition
  - 1997 – 2011
- IREX (Iris Exchange)
  - 1:1, 1:N Iris Recognition, Quality
  - 2008, 2010, 2011
- MINEX (Minutia Exchange)
  - 1:1 on card, 1:1 off card
  - 2005 – 2011
- SRE (Speaker Rec. Evaluation)
  - 1997 – 2011
- ELFT (Latent Fingerprint Tech)
  - 2007 – 2011
- PFT (Proprietary Templates)
  - 2003 – 2011

irex IRIS EXCHANGE

MINEX Minutia Exchange

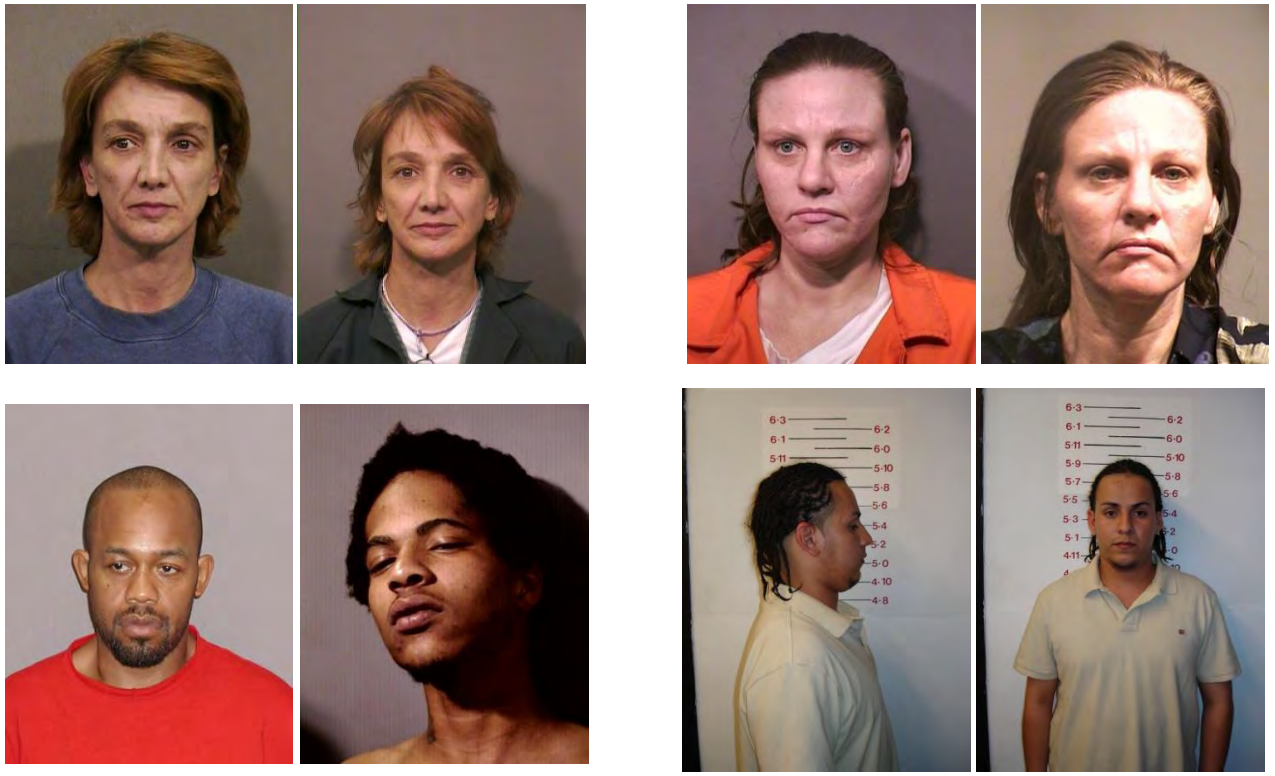
NIST

Chapter II :: Face Recognition

Selected Results from the 2D Still Image Track of the Multiple Biometric Evaluation

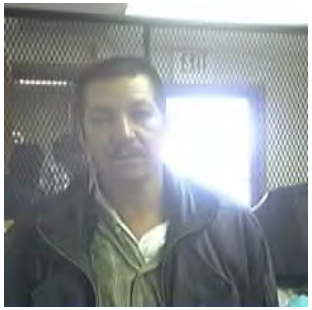
NIST

Law Enforcement (LEO) Images

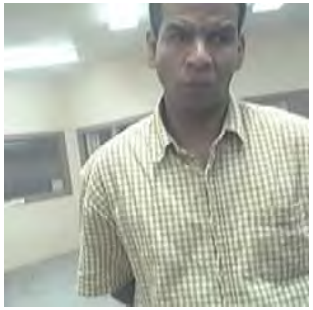


Fully public sample dataset is available: *Multiple Encounter Deceased Subject Database I+II*, NIST Special Database 32, December 2009.

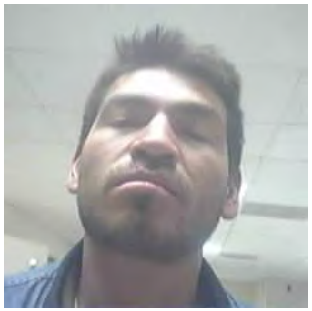
Webcam :: What mugshot standards?



Background impedes face detection and correct exposure of face



Subject too far from camera, gives low resolution.



Eyes closed?
Extreme pitch angle
Too close, gives distortion.

Cropped chin.
Photo-of-photo.
Scanning noise.

Detect and Fix During Capture

- Pose
- Facial expression
- Eyes closed

Detect and Cannot Fix Immed

- Camera + SOP
- Illumination (sometimes)
- Background (sometimes)
  - Need infrastructure mods

Not collected with any attention to mugshot standards.

ISO/IEC 19794-5 :2005+ Amd/1

ANSI/NIST ITL 1-2007, Annex H, Best Practice Recommendation For The Capture Of Mugshots, Version 2.0, September 23, 1997

NIST

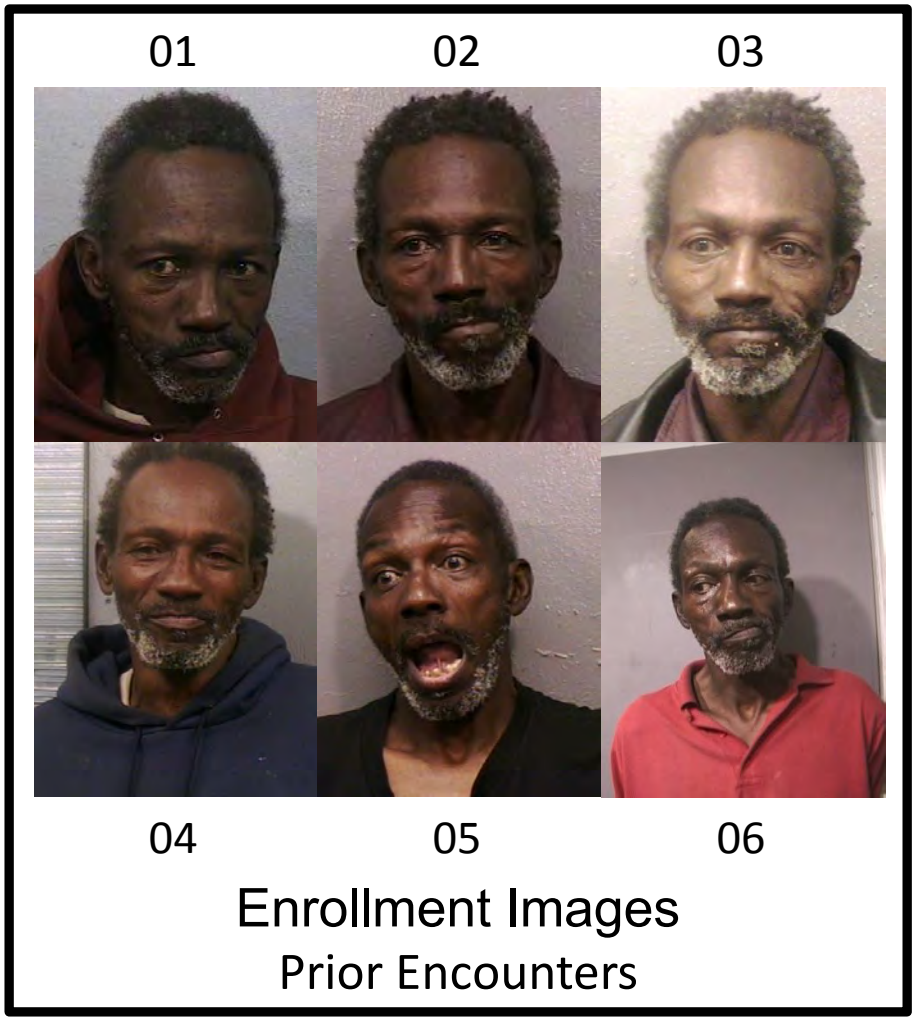
Accuracy Downside :: Webcam Images

1:N Accuracy, N = 1.6M Rank 1 Hit Rates	SDK	Photo File All	Photo File DHS Webcam	Photo File Without Webcam Estimated
L1	W22	0.88	0.54	0.93
MorphoTrak	Y21	0.83	0.39	0.89
Cognitec	X21	0.83	0.44	0.88
Pittsburgh Pattern Reco.	P22	0.65	0.35	0.69
NEC	V21	0.93	0.72	0.96

- Approx 12% of the MBE-STILL Photo File data are Webcam images.
- Error rates are 3 to 4 times higher on Webcam Images
- Second round MBE-STILL algorithms, N = 1600000

NIST

Multiple Encounters



07
Search Image
Last
Encounter

Vendor implemented (template-level) fusion

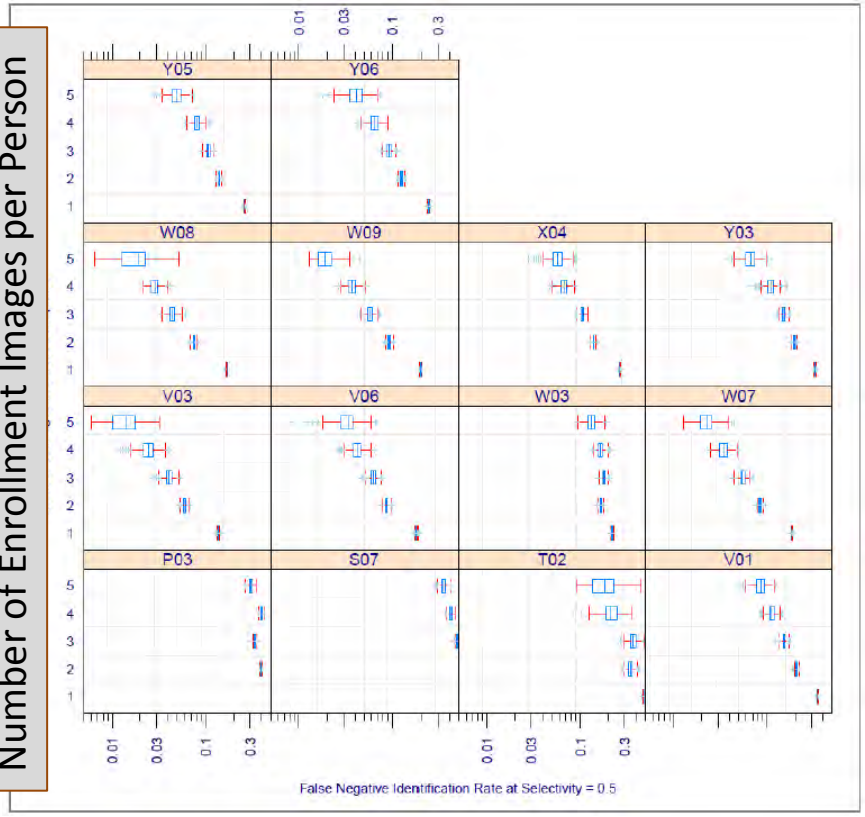
Template

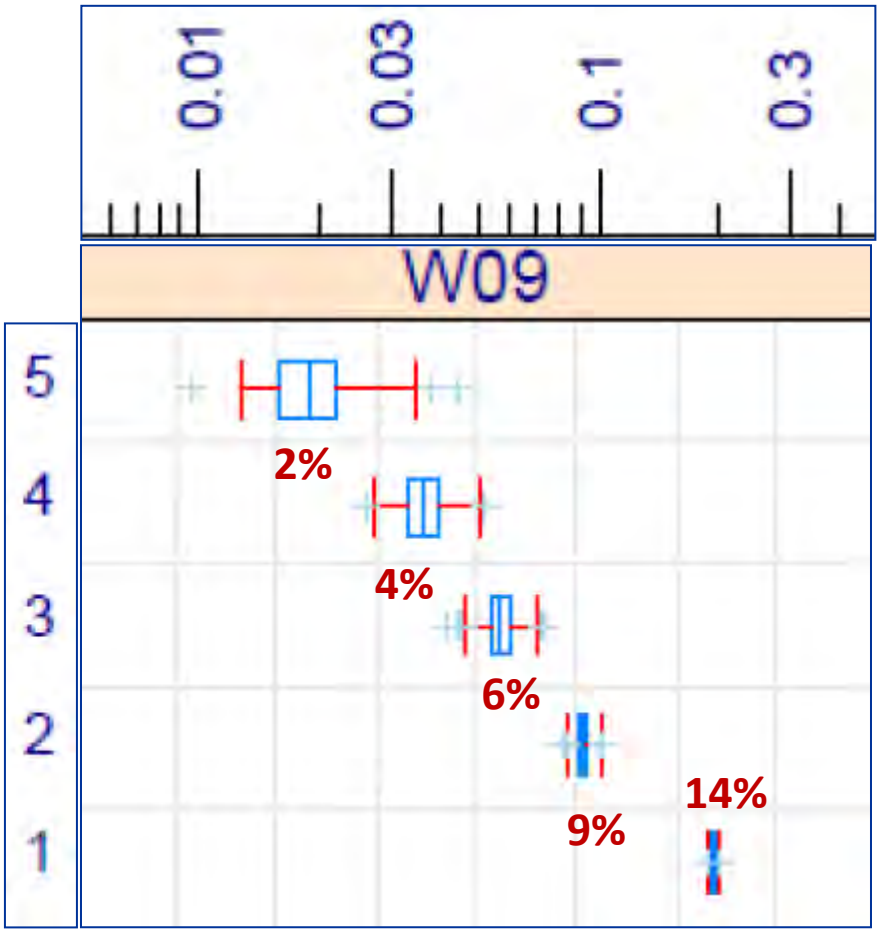
Template

Match

MEDS Example (S033)

Multiple Encounters: Miss Rate Reduction



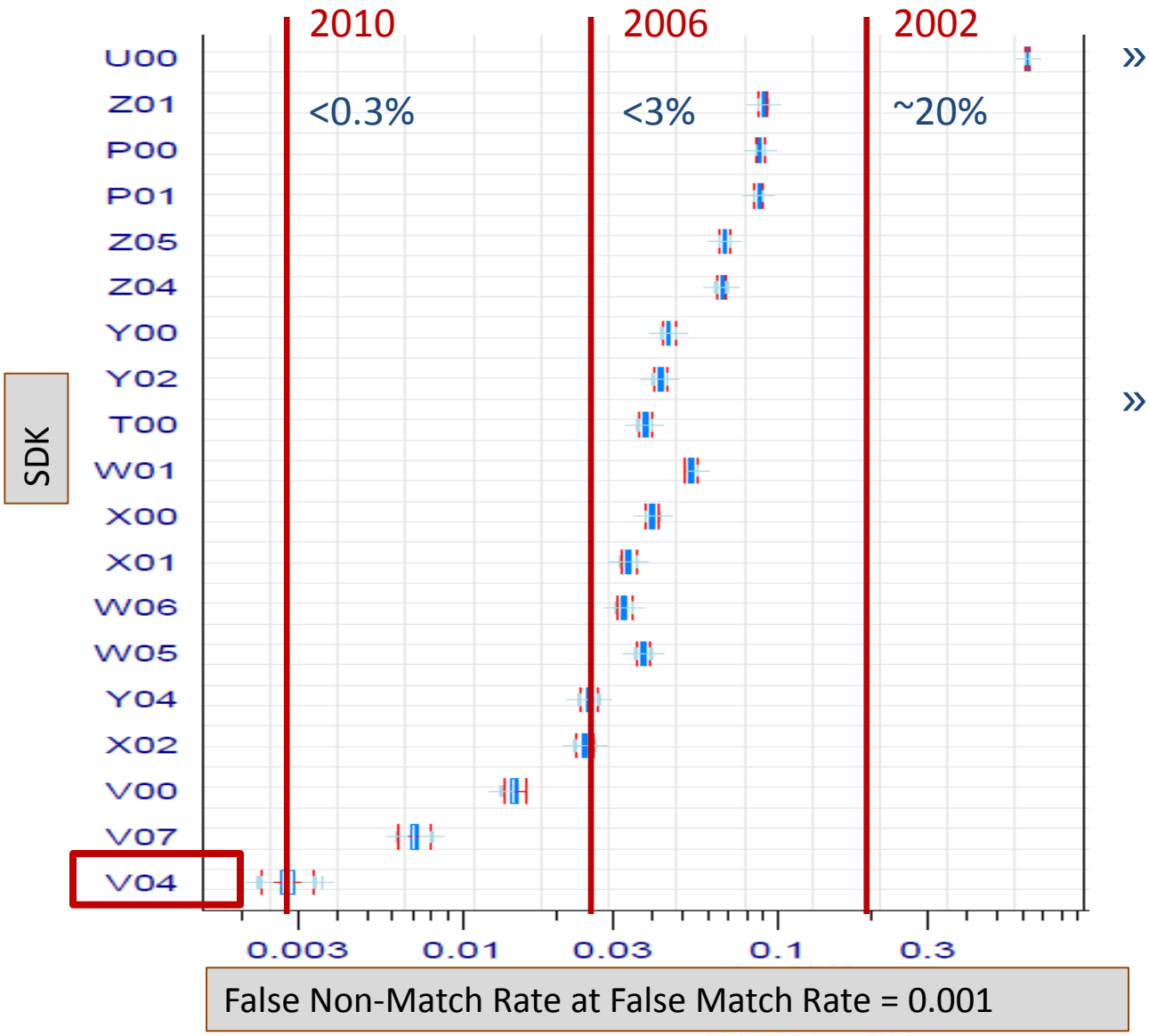


Enrolled Pop Size = 1.6M

Number of searches = 40K

Threshold set to give 0.5 false candidates per search, SEL(T) = 0.5

Fixed dataset used in three tests

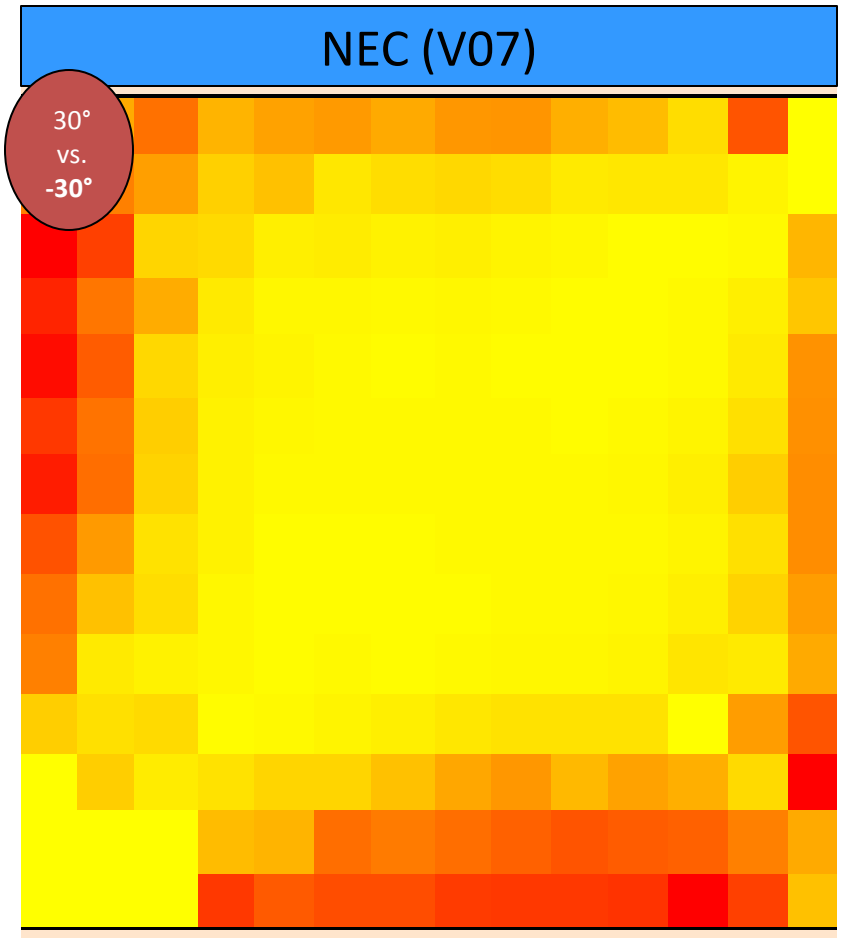


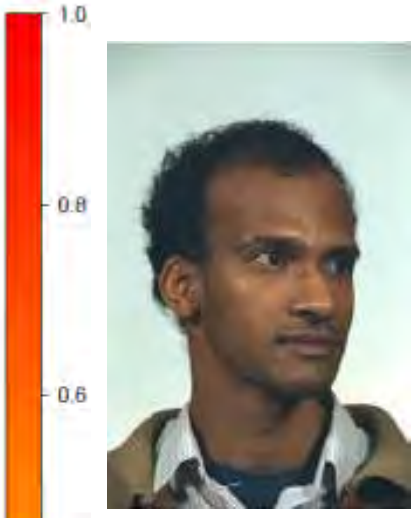
- Red lines show best prior results in
  - FRVT 2002
  - FRVT 2006
  - MBE 2010
- Images
  - DoS / FRVT 2002
  - 121589 images
  - 37437 persons
  - 300 x 352 image size
  - ~70 pixels eye-to-eye BUT
  - JPEG compressed ~10K

Cross-Pose Matching





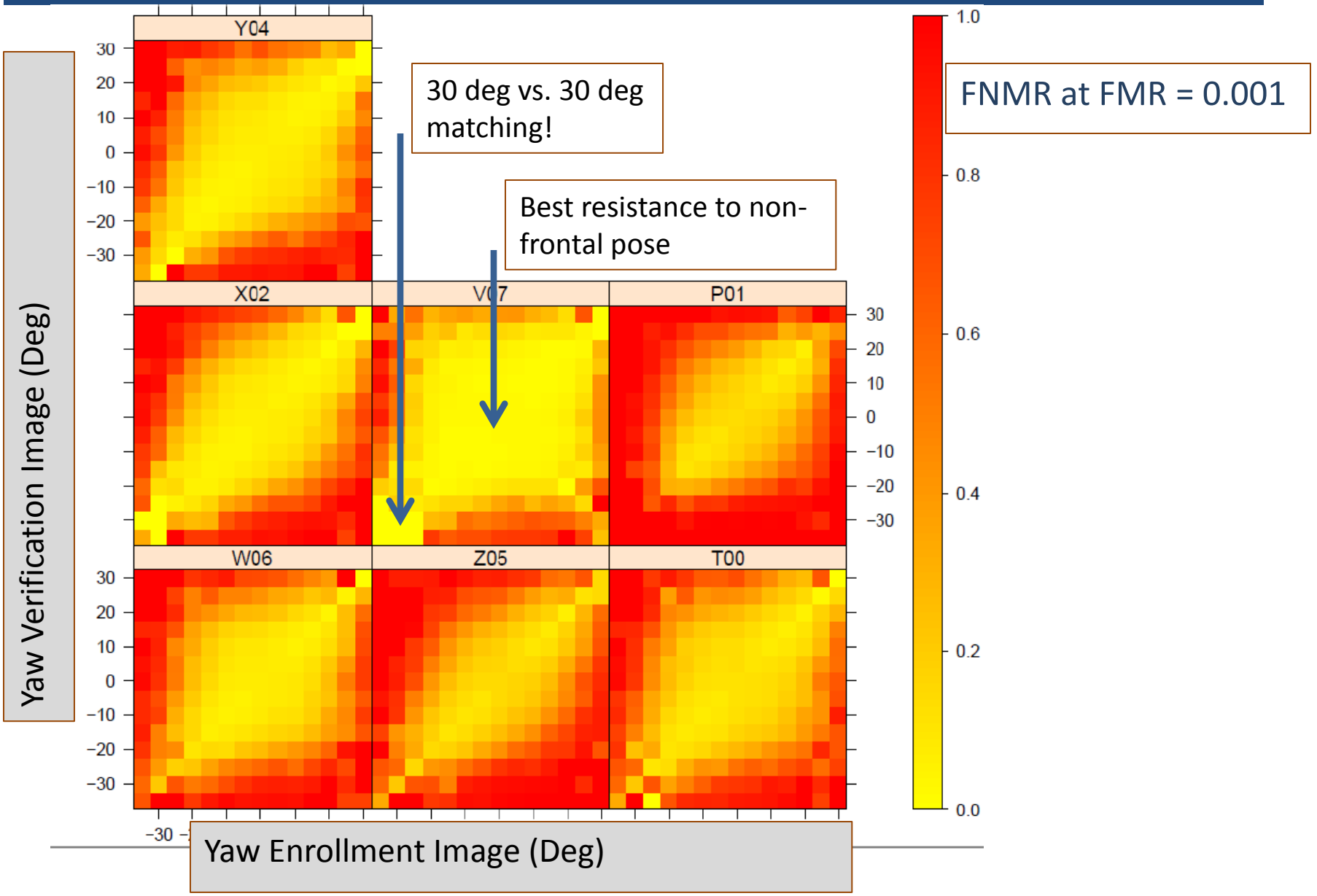




30° -30°

Matching Scenario

Cross-Pose Matching



Chapter III :: IREX

Selected Results from the Iris Exchange (IREX) Program Supporting IRIS Interoperability

NIST

Three IREX Activities

IREX I

- Formats, cropping, masking
- Compression limits
- Geometry, Margins, Radius
- Dilation, concentricity
- Concluded mid 2009
- Supported ISO/IEC 19794-6

IREX III

- 1:N with N in the millions
- One and two eyes
- Cross camera interop.
- Timeline
  - Started February 2011
  - Initial Report July 2011
- Open call for images

IREX II

- Iris Image Quality
  - Definition
  - Evaluation
  - Calibration
- Supporting ISO/IEC 29794-6
- Report Spring 2011

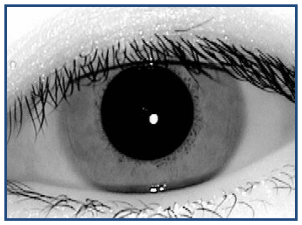
NIST

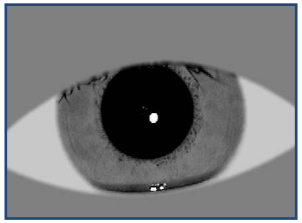
Compression + Format Recommendations

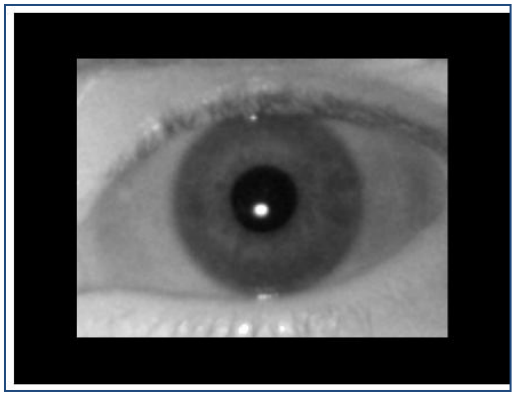
- Compression – Avoid it when you can!
  - Lossy compression does incremental damage to images.
  - Either no compression, or lossless may be sufficient.

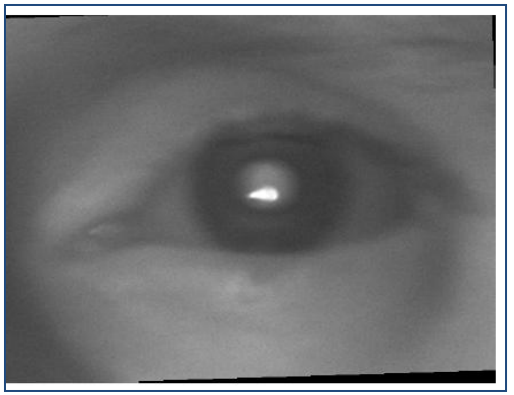
	Recommended		Target Record Size								
Role	Format	Compressor	2KB	4KB	8KB	16KB	32KB	64KB	128KB	256KB	307KB
All	KIND 1	Uncompressed									
All	KIND 3	Uncompressed									
All	KIND 7	Uncompressed									
All	KIND 3	PNG Lossless									
All	KIND 7	PNG Lossless									
1:N	KIND 3	JPEG 2000 Lossy									
1:N	KIND 7	JPEG 2000 Lossy									
1:1	KIND 3	JPEG 2000 Lossy									
1:1	KIND 7	JPEG 2000 Lossy									

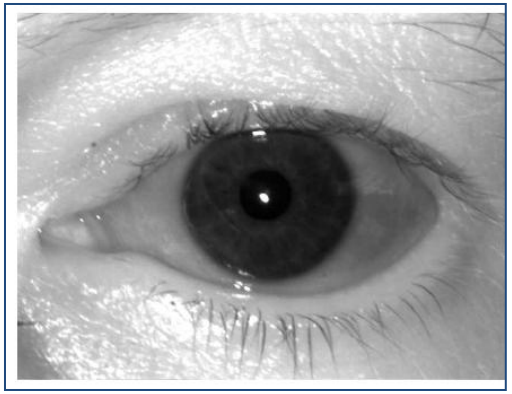
Irises :: One person, different images

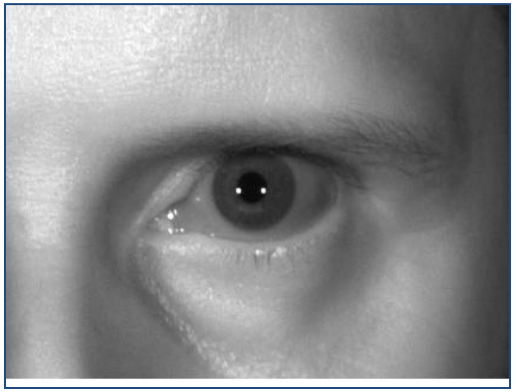


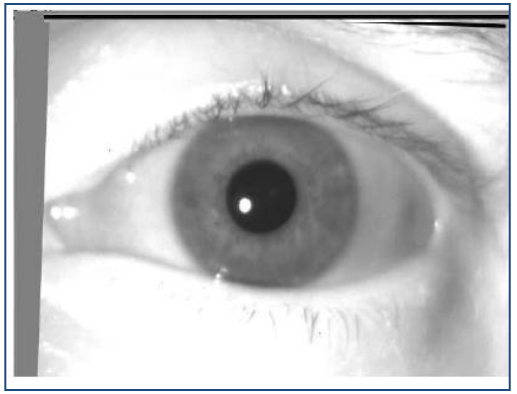






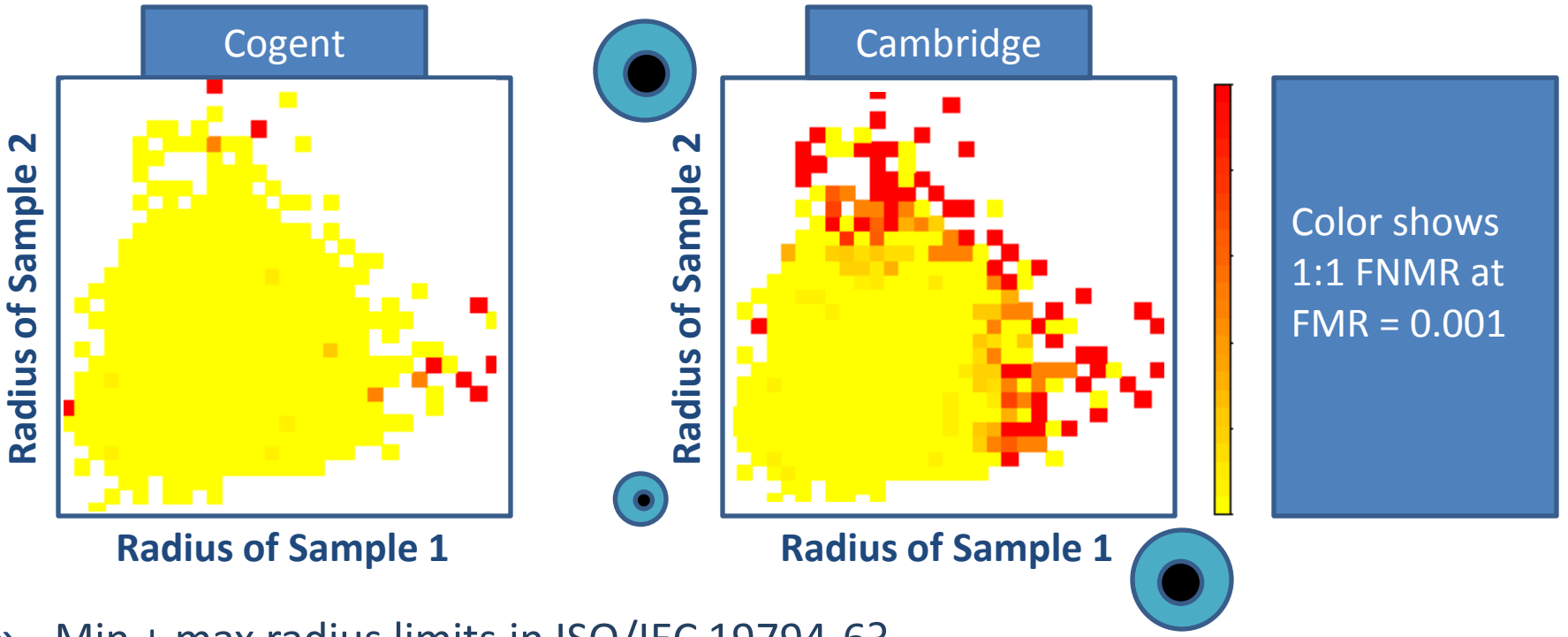






NIST

Iris Recognition :: Standardize Radius?



- Min + max radius limits in ISO/IEC 19794-6?
  - No, and the standard is nearing completion.
- In an application profile
  - Yes, in the US Gov PIV program, which will include iris, Fall 2010.

NIST

Figures from
http://iris.nist.gov/irex/irex_report.pdf.zip

Conclusions

- NIST conducts quantitative testing of biometric algorithms
  - Open, free, worldwide
  - Face, Finger, Iris, Speaker, Latent
  - Very large scale
  - Repeatable, fair
  - Independent
  - Operational data (often)
- NIST is active in biometric standardization
  - Face
  - Iris
  - Finger minutiae
  - Speaker
  - DNA
  - Image quality
  - SDO for ANSI/NIST ITL standard
  - Biometric Testing
  - Biometric Interfaces
- Active Test Programs
  - Face :: MBE-STILL
    - Updated MBE Report, Spring 2011
    - Compression Report, Spring 2011
  - MBE
    - Video
    - Face + Iris
  - MINEX II
    - Match-on-card, Imminent
  - Iris :: IREX II
    - Image Quality Report, Spring 2011
  - Iris :: IREX III
    - One-to-many Report, Summer 2011
  - Latent fingerprint
    - Phase II report, March 2011
    - Phase III ongoing, Report Late 2011
  - MINEX
    - Minutia Interoperability, Ongoing
  - PFT
    - End-stage-matchers, Ongoing

NIST

Links

- Feedback and further information:
  - patrick.grother@nist.gov
  - 301 975 4157
- ANSI/NIST Standard
  - Workshop March 1-3
  - http://fingerprint.nist.gov/standard
- Segmentation (SLAPSEG II)
  - http://fingerprint.nist.gov/slapsegII
- Minutiae (MINEX)
  - http://fingerprint.nist.gov/minex
- Match-on-Card (MINEX II)
  - http://fingerprint.nist.gov/minexII
- Latent Matching (ELFT)
  - http://fingerprint.nist.gov/latent
- Proprietary template fingerprint (PFT)
  - http://fingerprint.nist.gov/pft
- Iris Exchange Test 2008 (IREX)
  - http://iris.nist.gov/irex
- Video Face + Iris (MBGC)
  - http://face.nist.gov/mbgc
- Standards activity
  - A/N
  - http://fingerprint.nist.gov/standard
  - ISO
  - http://isotc.iso.org/livelink/livelink?func=ll&objid=8919152&objaction=ndocslist

NIST

BACK TO THE FUTURE!

Peter O'Neill
findBIOMETRICS.com
Feb 24, 2011

Who controls the past controls the **future**. Who controls the present controls the past.

George Orwell


BACK
TO
THE FUTURE

Data set-Participants

Participants include:
Iris ID Systems Inc.(formerly* LG Electronics), NEC, MorphoTrak, Lockheed Martin, Lumidigm, IBIA, Cross Match Technologies, Aware, AOptix, WCC, 3M, BIO-key, Accenture, e-DATA, MaxID, National Biometric Security Project, CSC, SmartMatic, Northrop Grumman, Merkatum, ZK Software, SAIC, *West Virginia University-Center for Identification Technology Research, IDTECK, Greenbit, Daon, San Jose State University, IEEE, Human Recognition Systems, Synochip, Airborne Biometrics Group, Avalon, Smart Sensors, TBS, Cognitec, Acuity, SecurLinx, Speech Technology Center, Suprema, HSB, Hanwang Technology, Triad, Time Management Inc, Wasp Barcode Technologies, C-True, Digital Persona, Fingerprint Cards, Hoyos Group, IdentiMetrics, Sonda, TAB, M2SYS, Integrated Biometrics, Secugen, SOFTPRO, Validity, Animetrics and UIDAI.

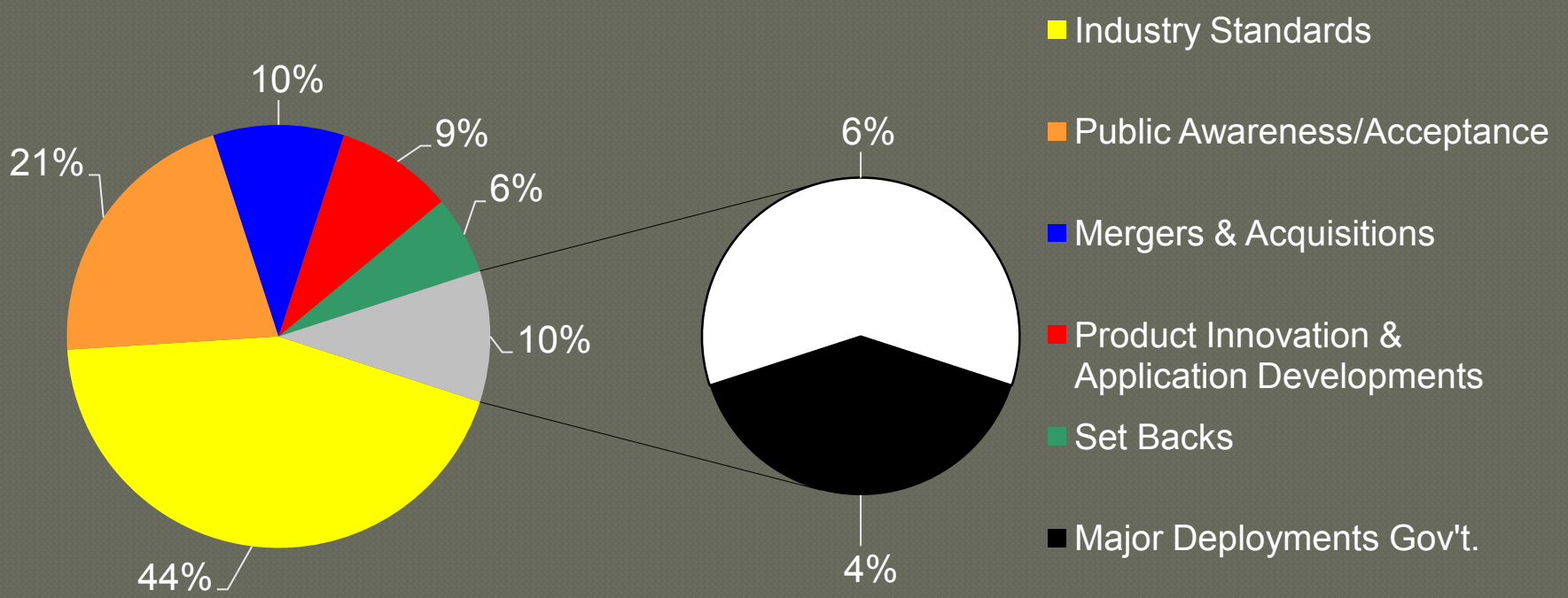
Global Perspective

Canada, India, Slovenia, Spain, Russia, Australia, China, Ireland, Brazil, Hong Kong, Sweden, Mexico, Germany, UK, Israel, France, Korea, The Netherlands, Lithuania, Singapore, Japan, Italy, Malaysia and the USA

In your view, what have been the three most significant milestones/announcements for the Biometric Industry this year?

Significant Milestones

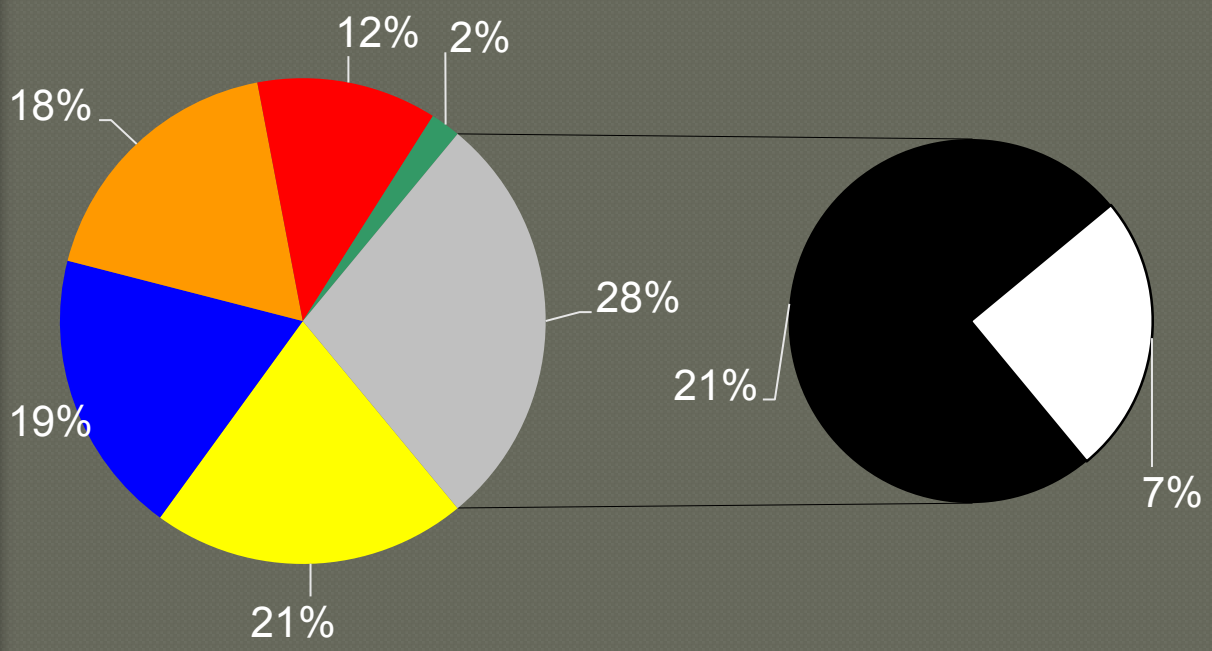
2004



findBIOMETRICS
Global Identity Management

Significant Milestones

2006

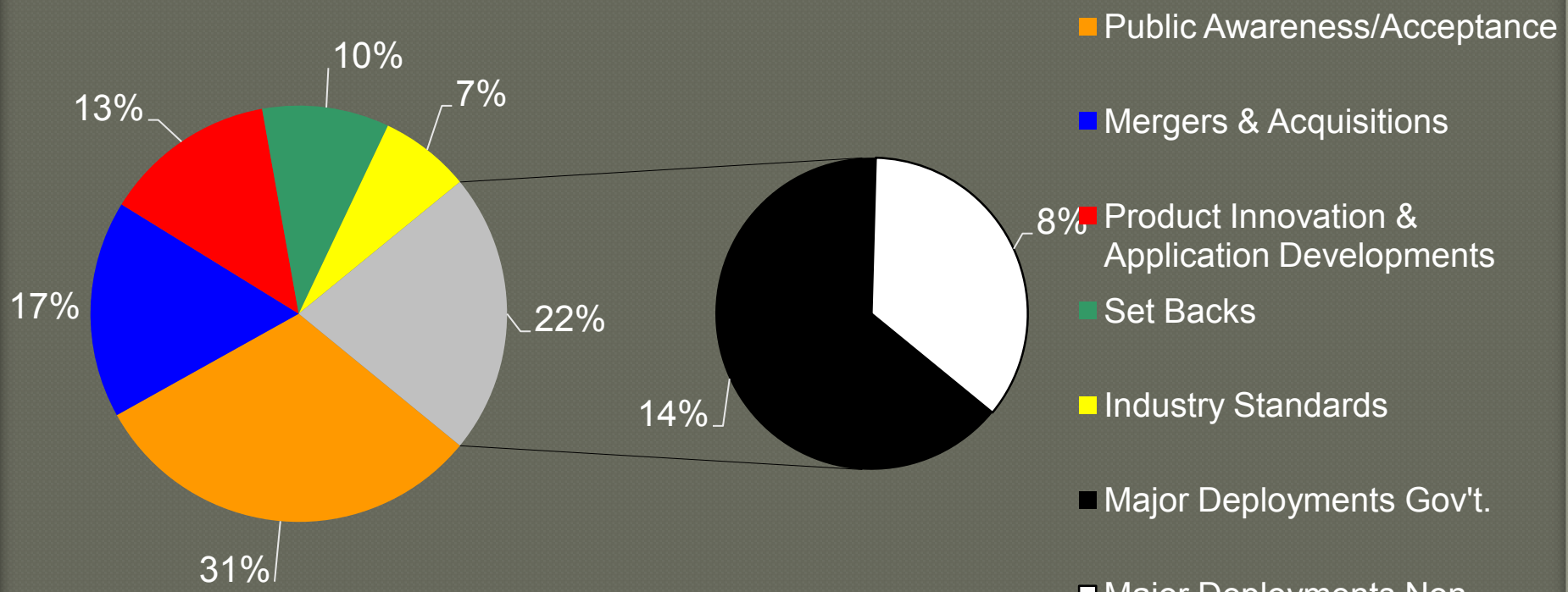


- Industry Standards
- Mergers & Acquisitions
- Public Awareness/Acceptance
- Product Innovation & Application Developments
- Set Backs
- Major Deployments Gov't.
- Major Deployments Non-Gov't.

findBIOMETRICS
Global Identity Management

Significant Milestones

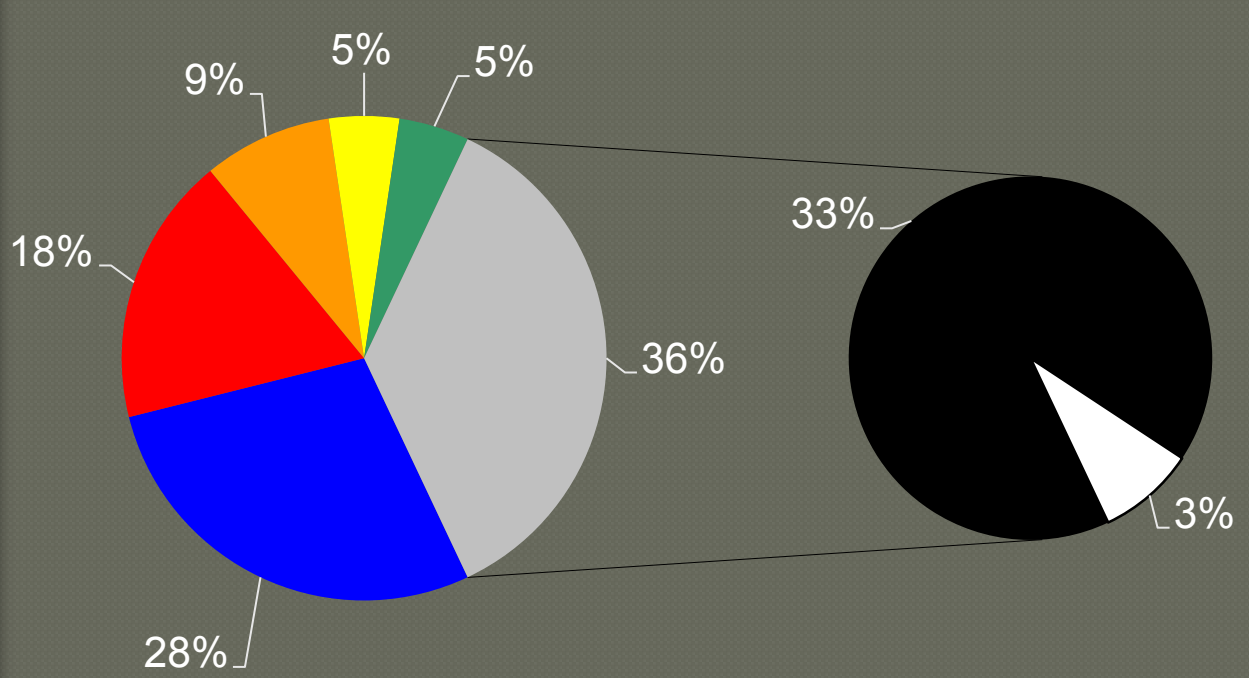
2008



findBIOMETRICS
Global Identity Management

Significant Milestones

2010

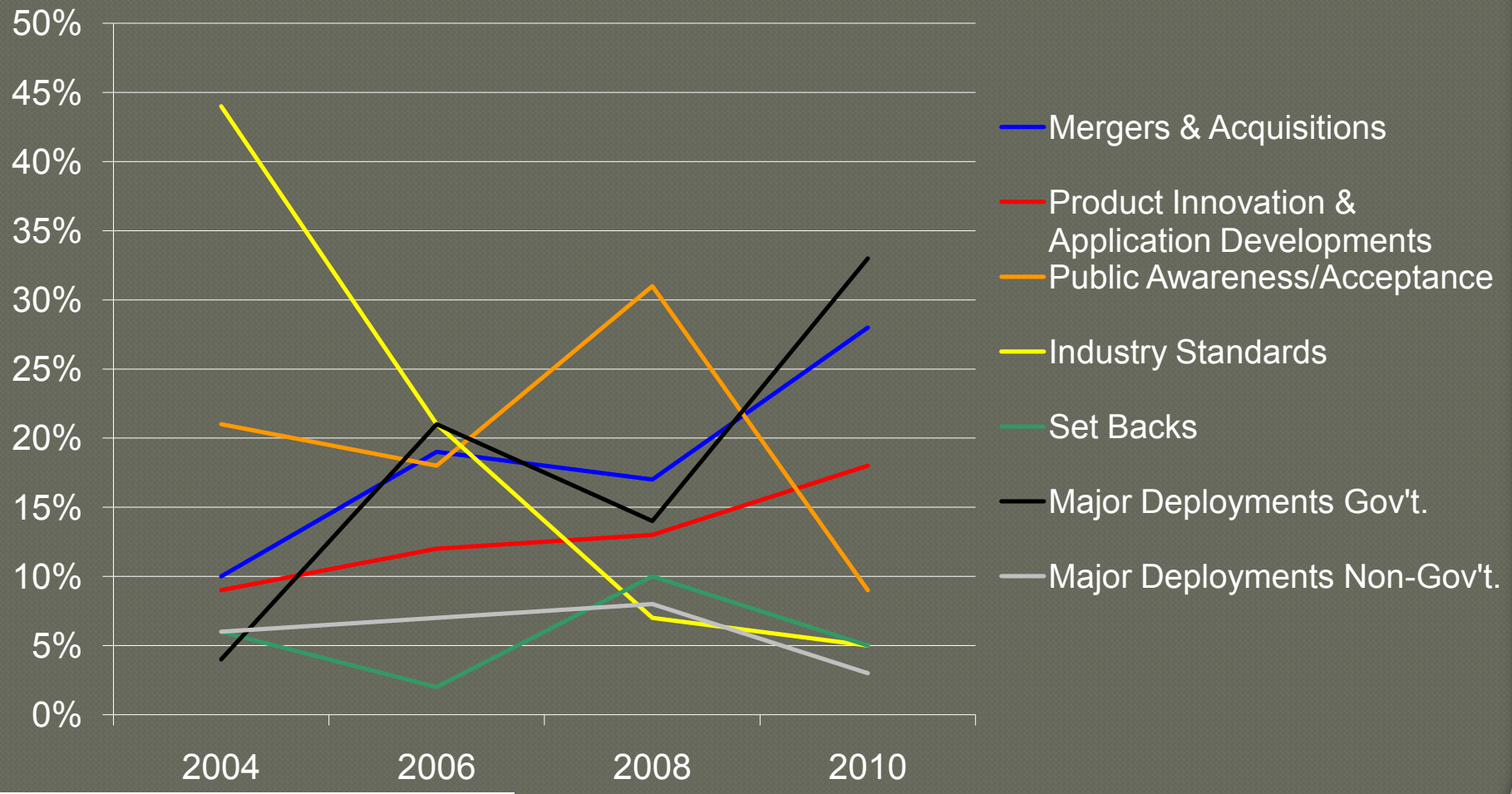


- Mergers & Acquisitions
- Product Innovation & Application Developments
- Public Awareness/Acceptance
- Industry Standards
- Set Backs
- Major Deployments Gov't.
- Major Deployments Non-Gov't.

findBIOMETRICS
Global Identity Management

Milestone Trends

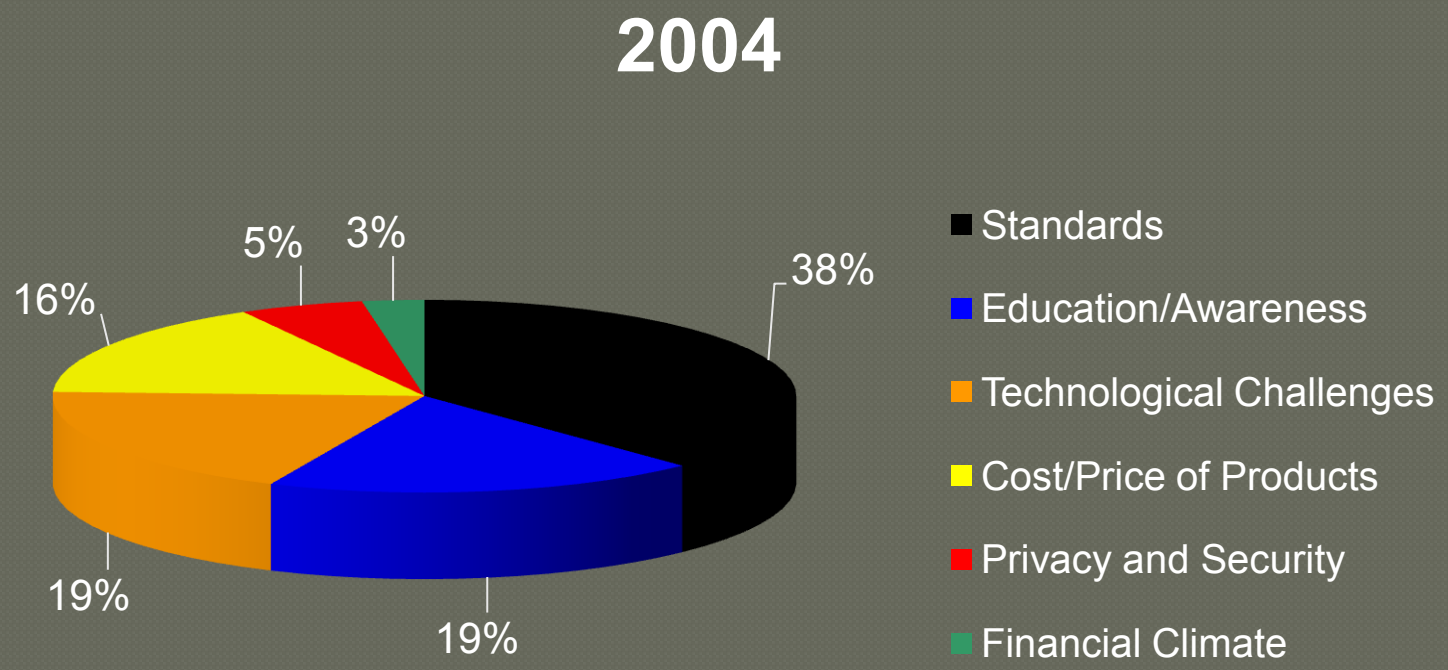
Note: Industry Standards, M&A, and Major Deployments



findBIOMETRICS
Global Identity Management

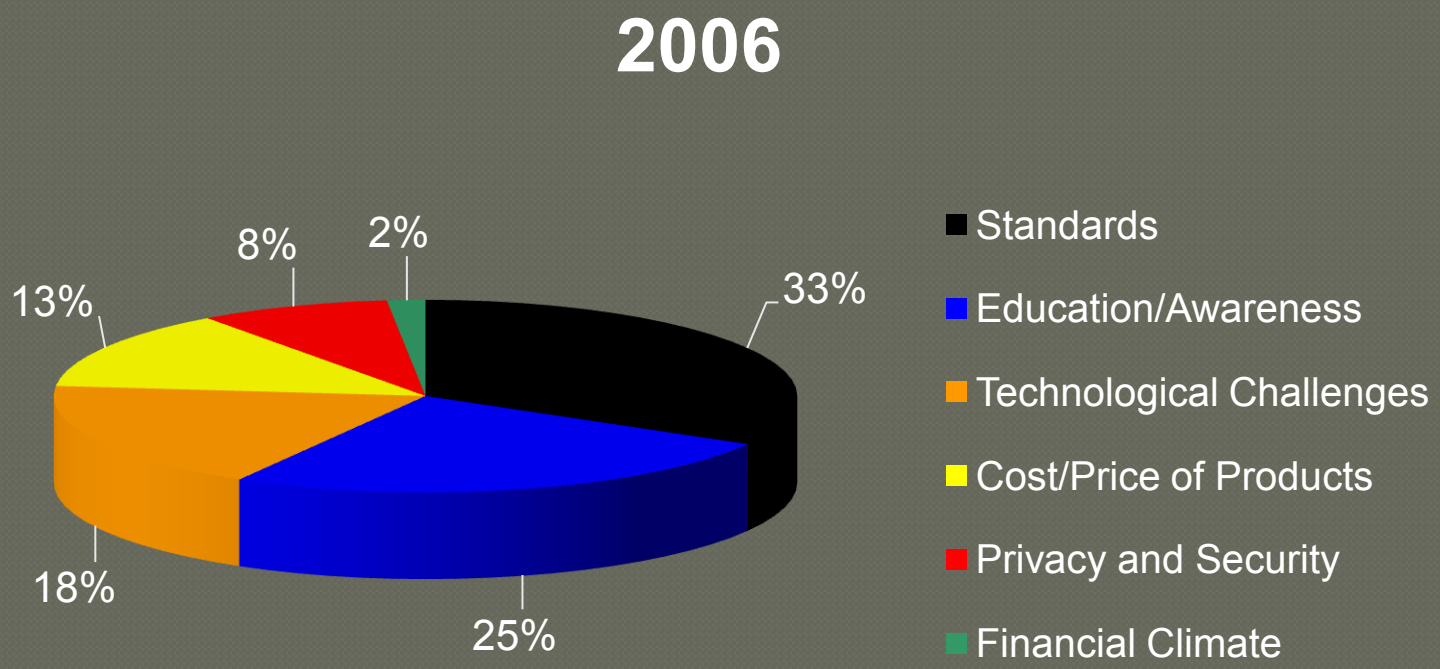
What are the most pressing issues facing the Biometric Industry as we move into the next year?

Issues Facing Biometric Industry



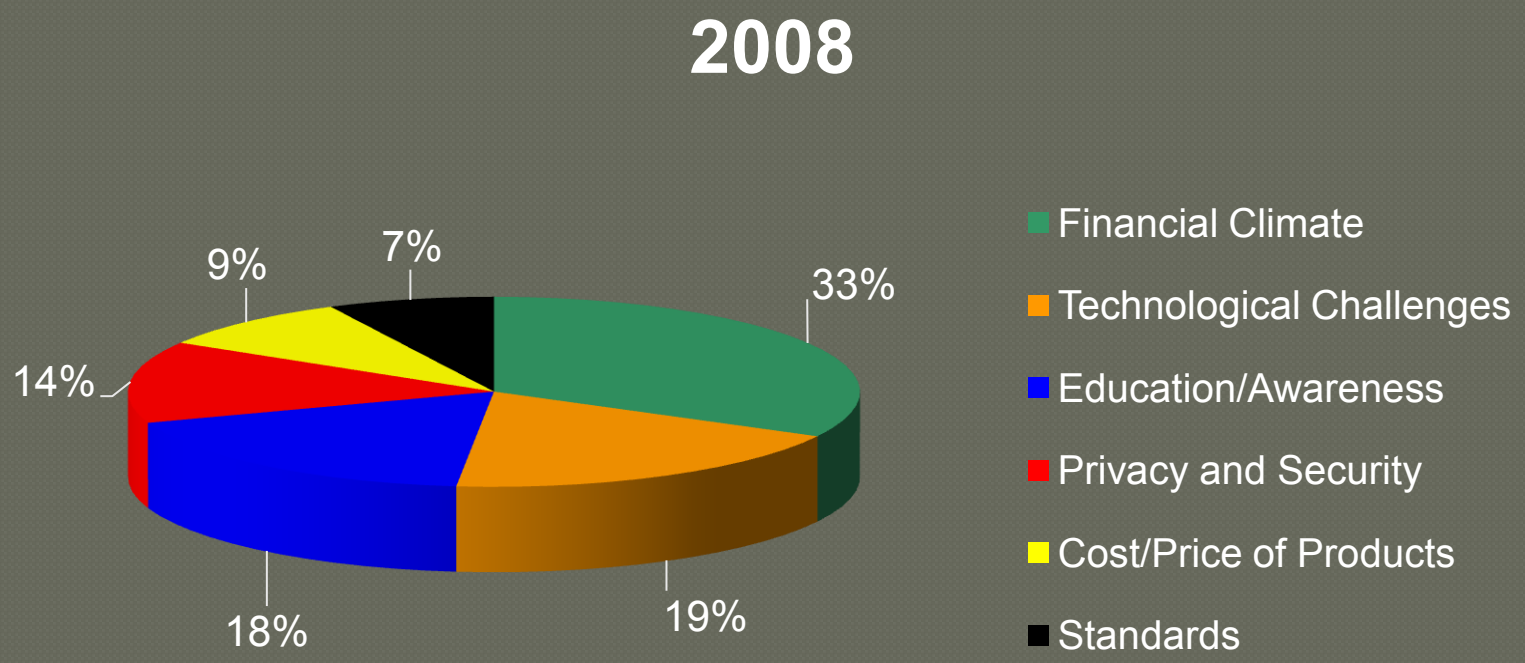
findBIOMETRICS
Global Identity Management

Issues Facing Biometric Industry



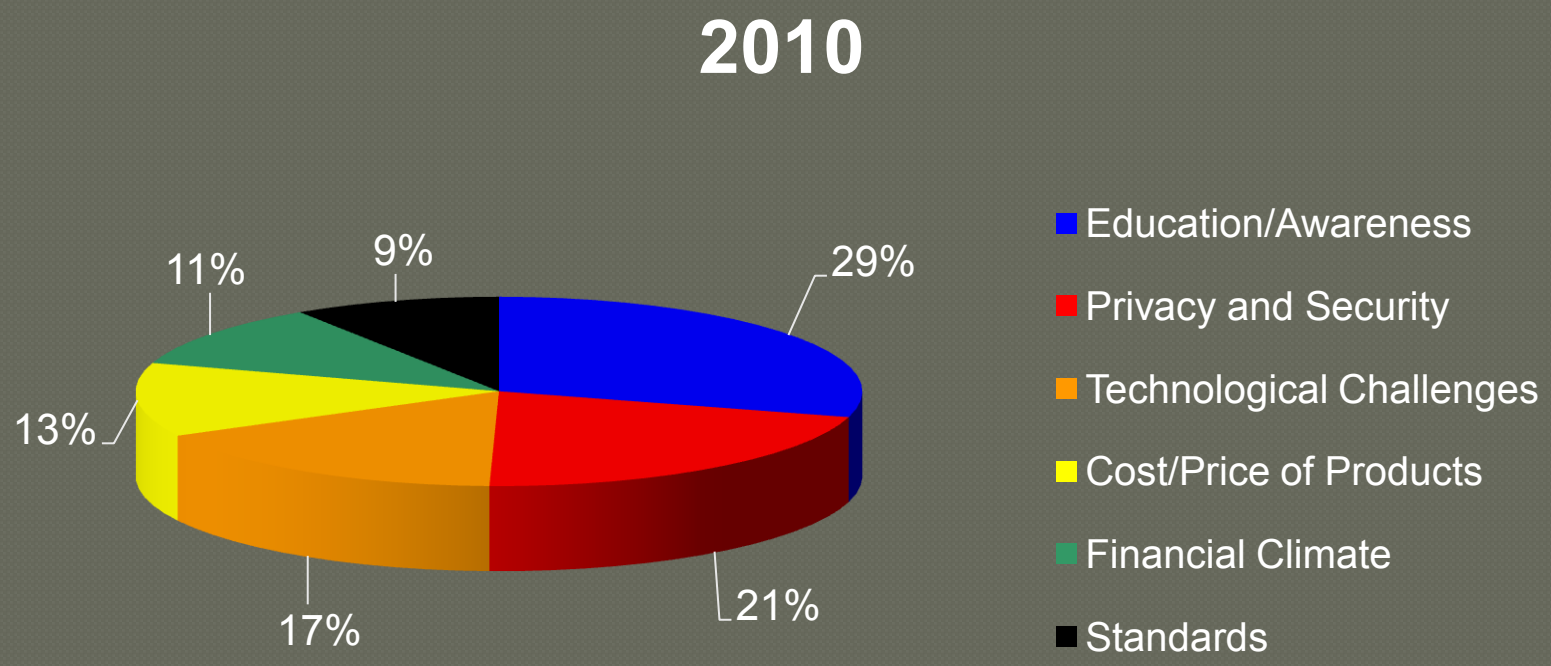
findBIOMETRICS
Global Identity Management

Issues Facing Biometric Industry



findBIOMETRICS
Global Identity Management

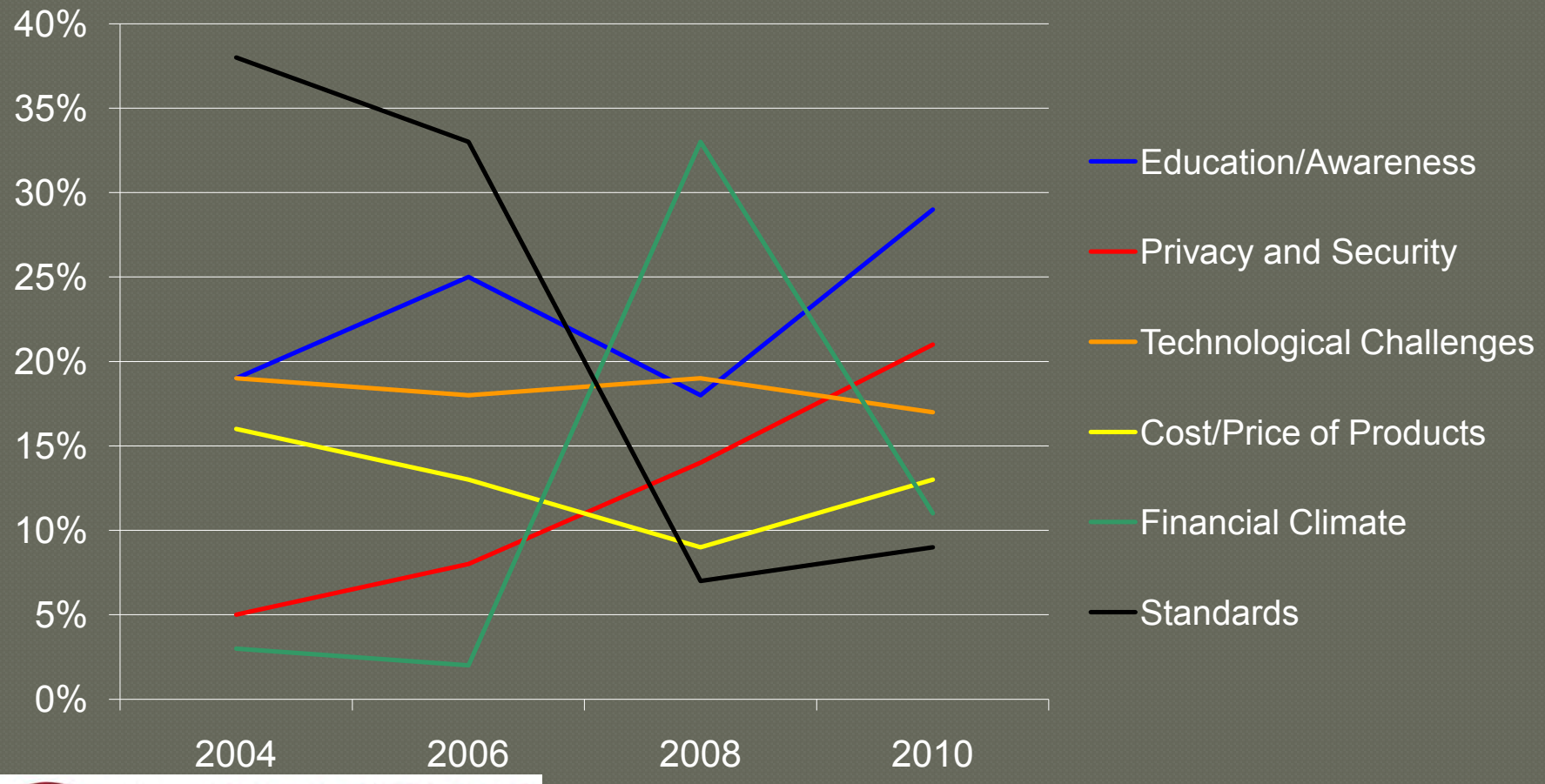
Issues Facing Biometric Industry



findBIOMETRICS
Global Identity Management

Changing Issues Facing Biometric Industry

Note: Standards, Education and Privacy



findBIOMETRICS
Global Identity Management

What's Next
The Future

Michael Delkoski, V.P., General Manager, 3M Security System Division.

You're asking, however, about what the future holds; and what we're counting on is that, over time, --and this is similar to GPS technology—that biometrics will migrate into many various verticals and a great many applications. There will be applications in the hospitality industry, in the financial industry, and I believe that you'll also see an increase in applications in building access sector. I am truly hoping that the technology, itself, will be able to drive itself down in costs, something similar to how GPS systems have.

The Future

What the experts are saying

The fledgling industry is poised for explosive growth over the next four years, owing in large part to continuing technological advances and a growing number of potential commercial and consumer applications.

findBIOMETRICS
Global Identity Management

The Future

HOWEVER, THIS IS WHAT THE EXPERTS WERE SAYING ABOUT GPS IN 1995!

The fledgling industry surrounding the **Global Positioning System** is poised for explosive growth over the next four years, owing in large part to continuing technological advances and a growing number of potential commercial and consumer applications.

The Future
THE GROWTH AREAS

- Mobile Applications
- Financial Service
- Health Care
- Online security
- Physical Access
- Automotive
- National ID Programs
- Homeland Security
- Travel
- Law Enforcement
- Time & Attendance
- Transportation
- Gaming
- Aviation
- Residential
- Hospitality

Let's take a look at just one area in more depth.

findBIOMETRICS
Global Identity Management

The Future

AT&T, VERIZON TO TARGET VISA, MASTERCARD WITH SMARTPHONES

- Mobile technology for banking and payments is reaching “a tipping point,” with younger consumers leading the way, Mercatus LLC, a Boston-based consulting firm, said in a June 7 study. More than half of U.S. consumers, and almost 80 percent of those between the ages of 18 and 34, will use mobile financial services within five years, according to Mercatus.
- “This is definitely a game-changer,” said industry consultant Richard Crone of San Carlos, California-based Crone Consulting LLC.

The Future

HOW APPLE AND GOOGLE WILL KILL THE PASSWORD

- AT&T and Verizon are not the only players interested in dominating this area.
- All Apple needs to do in order to turn the iPhone into a universal debit card is to add a tiny, inexpensive chip to the device. And all Apple needs to do in order to make the iPhone a universal secure ID is to add a fingerprint scanner to the phone and put another chip in its various desktop systems.
- The Android platform has also been at the forefront of workable biometric solutions for cell phones. In fact, you can already download Android apps that do face recognition and iris scanning.

findBIOMETRICS
Global Identity Management

The Future

This one example of the 16 that I showed earlier, illustrates the explosive growth potential of the Biometric Industry. Imagine layering on top of this growth potential the other 15 and you get an idea of where it could go and keep in mind what happened to GPS.

As a final note, keep an eye on the UIDAI Project (The Unique Identification Authority of India) in India. This is also a “game changer” for the industry!

Thank You

findBIOMETRICS.com

IBIA.org International Biometric and Identification Association

findBIOMETRICS
Global Identity Management

Homeland Security

US-VISIT

From the DIRECTOR

Since 2004, US-VISIT's innovative use of biometrics has strengthened our Nation's immigration and border management system to an unprecedented level. Today, our biometric identification services continue to transform how Government agencies protect our country from dangerous people by improving their ability to quickly and accurately identify the people they encounter and determine whether they pose a risk.

I'm proud of US-VISIT's support to decisionmakers on the front lines of homeland security as a single source of biometric and biographic information on criminals, immigration violators, and known or suspected terrorists. We touch almost every agency whose mission affects homeland security, from U.S. Customs and Border Protection officers at ports of entry, to the U.S. Coast Guard on the high seas, to local law enforcement agencies processing criminal aliens.

I'm pleased to report that in Fiscal Year 2010, with the support of Congress, US-VISIT contributed to key homeland security initiatives, including maturing our organization, advancing our interoperability capabilities with the Federal Bureau of Investigation and the Department of Defense Biometric Identity Management Agency, investing in new technologies, and expanding collaboration with our domestic and international partners. I call it a "bridge year" that built on what we've achieved and sets a firm foundation for moving forward on ambitious goals.

Fiscal Year 2010's groundwork will allow US-VISIT to optimize our accomplishments in the year ahead. We'll significantly increase the size and accuracy of our US-VISIT biometric watchlist, keep pace with growing volumes of travelers, test new technologies in operational environments, and meet increasingly sophisticated threats. We'll focus on maximizing managerial efficiencies, growing our workforce, and building out new office space in Arlington, Baltimore, and San Diego. So we'll continue to grow and expand as an organization over time to meet the mission-critical needs of the Department.

This report highlights our achievements and outlines our priorities for Fiscal Year 2011 so that we can continue to deliver innovative identification and analysis services to help keep our Nation safe.

Cordially,

Robert A. Mocny
Director

WHAT'S IN SIDE

ACCOMPLISHMENTS

SUSTAINED AND EXPANDED INTERNATIONAL PARTNERSHIPS

In collaboration with its global partners, US-VISIT developed common biometric standards and best practices to share information about criminals, immigration violators, and known or suspected terrorists.

US-VISIT deepened existing partnerships with the United Kingdom, Australia, and Canada, and forged new partnerships with New Zealand, India, South Africa, the Republic of Korea, Germany, Spain, Greece, and the Dominican Republic to support their implementation of biometrics in border and immigration control.

In conjunction with Visa Waiver Program (VWP) countries that have signed Preventing and Combating Serious Crime (PCSC) agreements with the Department of Homeland Security and the Department of Justice, US-VISIT developed a process for technical implementation. Working with Germany's Ministry of the Interior, U.S. Immigration and Customs Enforcement (ICE), and the Federal Bureau of Investigation, US-VISIT developed technical standards for implementing PCSC agreements with other VWP countries. Discussions are underway with Spain and the Republic of Korea to develop business processes and technicals solutions for reciprocal biometric and biographic information exchanges.

US-VISIT provided technical assistance to Mexico's National Institute for Migration to facilitate the incorporation of biometrics into its Integrated System for Migration Operations as envisioned under the Mérida Initiative. This project is a collaborative effort among the United States, Canada, and Mexico under the Security and Prosperity Partnership of North America. The partnership focuses on combating transnational crime and confronting organizations whose illicit actions undermine public safety, erode the rule of law, and threaten national security. Sustained collaboration will facilitate the exchange of actionable biometric information between these countries.

Through the Five Country Conference, the United States, Canada, Australia, New Zealand, and the United Kingdom continued to build an automated information exchange capability to screen immigration-benefit seekers and violators in real time. US-VISIT seconded technical experts to Canada, Australia, and the United Kingdom to assist in building and deploying biometric capabilities.

SUPPORTED SECURE COMMUNITIES INITIATIVE

US-VISIT supported the expansion of ICE's Secure Communities. Interoperability of US-VISIT's Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) is the cornerstone of ICE's Secure Communities strategy to better identify and remove criminal aliens from the United States and to transform overall alien enforcement efforts. By the program's second year, local law enforcement agencies in numerous jurisdictions nationwide were able to check fingerprints of arrestees against IDENT and IAFIS during the booking process. In FY 2010, US-VISIT supported the expansion of this capability to additional jurisdictions.

COLLABORATED WITH U.S. CUSTOMS AND BORDER PROTECTION

In FY 2010, US-VISIT delivered a key component that supports the Electronic System for Travel Authorization (ESTA) Program and the elimination of the paper arrival-departure form (Form I-94W). US-VISIT worked closely with U.S. Customs and Border Protection (CBP) to ensure US-VISIT's Arrival and Departure Information System (ADIS) could provide departure-matching information to CBP for ESTA-approved VWP travelers on carriers and at selected ports of entry (POEs). This enabled CBP to electronically validate the departure of VWP travelers, eliminating the need for a paper I-94W form. To date, ADIS has matched and sent information on 17,000 departures to CBP for this program.

EXPLORED NEW TECHNOLOGIES IN AN OPERATIONAL ENVIRONMENT

In FY 2010, US-VISIT tested and evaluated iris and facial recognition capabilities in an operational environment. As iris and facial recognition technology matures, it is critical to understand its capabilities and limitations in operational settings and to evaluate what additional development may be required to reduce acquisition risk.

US-VISIT and the DHS Science and Technology Directorate co-sponsored an Iris-Face Technology Demonstration and Evaluation in McAllen, Texas, in October 2010. This was an operational test of prototype iris-face capture to assess the technology's viability and potential effectiveness in supporting DHS operations.

The test analyzed data in multiple areas, including image quality, iris anomaly effects on matching, and the performance of cross-camera image matching. It also recorded instruction time, failure rates, and acquisition time for an operational DHS component. US-VISIT continued its biometric technology innovation by evaluating additional biometric modalities for incorporation into the existing fingerprint identification system. These modalities included iris, face, palm prints, scars, marks, tattoos, and DNA profiles.

The field trial was conducted at the McAllen Border Patrol Station in the Rio Grande Valley Sector. This site was selected for the test and for US-VISIT's Multimodal Limited Production Pilot because a high volume of illegal immigrants from multiple countries are apprehended there. The pilot includes Border Patrol and Global Entry.

EXECUTIVE STAKEHOLDER BOARD

US-VISIT continued to improve its customer service with more direct collaboration at the strategic level through the Executive Stakeholder Board. This group provided a forum for discussing how US-VISIT's services can or should be adapted to fit the needs of its partners and enables US-VISIT to better serve its customers at a strategic level.

BEHIND THE SCENES

In addition to reaching important milestones in FY 2010, US-VISIT accomplished many internal goals to ensure continued program success, including the following:

- Adhered to key performance targets relating to quality, timeliness, and systems availability to customers.
- Achieved cost and schedule efficiency targets, staying within the earned-value parameters established for the fiscal year.
- Increased the US-VISIT Federal workforce during FY 2010 by nearly 40 percent. In alignment with the DHS Balanced Workforce Initiative, US-VISIT hired 96 new Federal employees.
- Implemented a Biometric Education Strategic Plan in partnership with CBP. This plan resulted in training on US-VISIT biometric watchlist management and basic biometric issues for CBP officers to improve their ability to capture biometrics, while simultaneously enhancing the quality of biometric data for IDENT processing.
- Developed a technical reference document on biometric standards to which US-VISIT currently conforms or will implement in the near term to support new biometric technologies and services, and to enhance interoperability with its domestic and international partners.
- Received the highest security rating from the Office of Management and Budget (OMB), based on Federal Information Security Management Act criteria.

US-VISIT IN ACTION

US-VISIT's biometric identification and analysis services help Federal, State, and local decisionmakers accurately identify the people they encounter and determine whether those people pose a risk to the United States.

Decisionmakers use these services to enhance:

- International traveler screening at ports of entry (POEs) and visa-issuing posts
- Immigration-benefit applicant screening
- Immigration enforcement at sea, along the land borders, and within the interior of the country
- Law enforcement and terrorism investigations

The percentage of IDENT transactions in FY 2010, by customer, included the following:

- **CBP: 71 percent**
- **Department of State (DOS): 13 percent**
- **FBI: 9 percent**
- **U.S. Citizenship and Immigration Services (USCIS): 4 percent**
- **ICE and CBP enforcement: 3 percent**
- **Department of Defense (DOD), the Coast Guard, and United Kingdom Border Agency (UKBA): <1 percent**
- **Transportation Security Administration (TSA): <1 percent**

In FY 2010, US-VISIT processed 60 million biometric identification and verification transactions for customers, a 17 percent increase over FY 2009.

The average US-VISIT biometric watchlist search time to return a response about a traveler at any POE was six seconds in FY 2010.

The average search time to return a response about a visa applicant at any consular office was 3.14 minutes.

Biometric matches to the US-VISIT biometric watchlist in FY 2010 included 6.5 percent in enforcement encounters, 6.7 percent for immigration benefits, 9.4 percent for border crossing cards and visa applications, and 21.7 percent at CBP POEs. DOD and DOJ matches (55.7 percent) comprised the largest percentage of matches in FY 2010.

ADIS, US-VISIT's biographic system, is the only information system in the Federal government that can provide visa overstay data. Its primary benefit is the identification of persons who are in-country or out-of-country overstays, either by providing recommended leads to ICE or by promoting individuals to the US-VISIT biometric watchlist. Overstay data can result in investigations and deportations by ICE, the denial of visas by the Department of State, or the denial of entry at POEs by CBP.

At the end of FY 2010, ADIS contained the travel histories of approximately 167 million alien travelers. From FY 2009 to FY 2010, ADIS unique-person identity records increased by approximately 22 million and are expected to grow at an annual rate of 25 million records.

Biometric Support Center

The primary mission of **US-VISIT's Biometric Support Center (BSC)** is to provide expert fingerprint verification in support of stakeholder operations when automated means are not sufficient. Every day—24 hours a day, seven days a week—highly trained fingerprint examiners perform urgent comparisons to quickly verify fingerprints that either match a US-VISIT biometric watchlist record or cannot be verified by US-VISIT's automated matching system. DHS components use this information to facilitate admissibility and criminality determinations as well as benefit and credentialing eligibility decisions.

The BSC also provides expertise and support to Federal, State, local, tribal, and international law enforcement agencies, intelligence agencies, and foreign governments that submit latent or rolled fingerprints to US-VISIT for identification. The agencies then use this information to solve crimes, support terrorist investigations, and identify unknown deceased persons. BSC examiners have also served as expert witnesses in trials across the Nation.

Did You Know?

FY 2010

- **BSC fingerprint examiners completed 185,866 urgent fingerprint comparisons, averaging just over four minutes per verification.**
- **As a result of 10-print upgrades, all 10-prints received by US-VISIT are run against the latent prints file. Latent print examiners completed over 5.1 million latent print comparisons, resulting in 149 identifications.**
- **The BSC identified 242 unknown deceased persons, amnesia victims, and others.**

Mission Support Services

US-VISIT's Mission Support Services (MSS) is a recognized source for timely, relevant, and credible information on entry, exit, and immigration overstay status. It strives to become the innovator and catalyst for the integrity of mission systems data in direct support of US-VISIT's goals of enhancing security, facilitating legitimate trade and travel, ensuring the integrity of the immigration system, and protecting the privacy of our visitors. MSS analyzes ADIS-generated records of interest and provides validated overstay information to DHS operational units that use US-VISIT entry, exit, and status data to enforce immigration laws.

MSS identifies system- or human-generated data integrity issues to improve the quality of US-VISIT information in IDENT and ADIS. In addition, MSS reviews US-VISIT biometric watchlist encounters and adjudicates the promotion or demotion of persons to or from the US-VISIT biometric watchlist based on the most current information associated with an individual.

Adjudications are conducted to ensure that the US-VISIT biometric watchlist continues to be accurate and actionable for all US-VISIT stakeholders. MSS also performs ad hoc compliance studies for internal DHS organizations and the Department of State.

Did You Know?

FY 2010

- **MSS exceeded its goal of validating 50 percent of the one million records that comprised the previously unvetted population by validating 580,000 records.**
- **MSS nearly doubled the number of leads sent to ICE, from 16,379 in FY 2009 to 30,406 in FY 2010, resulting in 514 arrests of in-country overstay violators.**
- **MSS conducted over 205 validation studies for the Department of State's Fraud Prevention Unit.**
- **US-VISIT biometric watchlist adjudications in FY 2010 totaled 94,575, exceeding FY 2009 production by more than 300 percent.**

Reporting and Analysis

US-VISIT's Reporting and Analysis Services (RAS) provides operational research and coordination on all current and future US-VISIT international and domestic biometric and biographic information-sharing initiatives, including Preventing and Combating Serious Crime agreements scheduled for implementation in 2011 and current sharing initiatives with the United Kingdom, Canada, Australia, and New Zealand. These efforts enable US-VISIT to collect, maintain, and share biometric and biographic information with international and domestic customers to identify mala fide aliens entering the United States or individuals who may pose a threat to the country.

RAS provides operational, identity management, and systems information in daily, weekly, quarterly, and annual reports to Congress, DHS, the National Protection and Programs Directorate, and US-VISIT senior management. RAS is developing the capability to provide the intelligence and law enforcement communities with Homeland Intelligence Reports on biometric, biographic, and identity fraud analyses of the vast amount of identity information in US-VISIT's systems.

RAS also works with the law enforcement and intelligence communities to ensure that individuals who may pose a threat to United States national security or who may be inadmissible to the country are included in the US-VISIT biometric watchlist available to all customers.

Did You Know?

FY 2010

- **Coordinated with United Kingdom Border Agency on 164 US-VISIT biometric watchlist matches, providing shareable DHS information.**
- **Coordinated with Five Country Conference partners and shared data on over 68 asylum/refugee cases, resulting in the denial of five cases overseas and three in the United States, the identification of four overseas known or suspected terrorist cases, and the referral of six cases to the United States immigration judge for removal considerations.**
- **Compiled and analyzed over 100 data analysis reports for US-VISIT management and DHS components.**
- **Promoted 866 known or suspected terrorists to the US-VISIT biometric watchlist based on information received from the intelligence community and other partners.**

U.S. Citizenship and Immigration Services

U.S. Citizenship and Immigration Services uses US-VISIT's services to establish and verify the identities of people applying for immigration benefits, including asylum or refugee status.

Did You Know?

FY 2010

- **US-VISIT established or verified the identities of 2,040,000 applicants for immigration benefits—more than 5,500 a day.**
- **Immigration benefit applicants accounted for 6.7 percent of all US-VISIT biometric watchlist matches.**

U.S. Coast Guard

Based on existing threats in early 2010, the **U.S. Coast Guard** began to biometrically identify the crews of liquefied natural gas tankers being loaded in the port of Balhaf, Yemen, to ensure the crews on the tankers do not pose a security risk. In a collaborative effort among US-VISIT, the Department of State, Department of Defense, and the Coast Guard, biometric and biographic data is collected from and submitted to the appropriate Government databases. The crews' fingerprints are also loaded into a mobile biometric device that the Coast Guard uses to verify each crew member's identity once the vessel reaches U.S. waters.

The Coast Guard employs US-VISIT's biometrically based services at sea to apprehend and prosecute illegal migrants and migrant smugglers. The Coast Guard relies on mobile biometric collection devices—handheld scanners and cameras—to collect and compare migrants' biometric information against information in the US-VISIT database about criminals and immigration violators.

Did You Know?

FY 2010

Since the Coast Guard began collecting biometrics from illegal migrants at sea, illegal migration in the area where the technology is being used has dropped by at least 80 percent.

U.S. Customs and Border Protection

US-VISIT supports **CBP's** Office of Field Operations by verifying the identities of international travelers each day at ports of entry (POEs), helping them determine whether a non-U.S. citizen arriving at one of our ports should be admitted to the country. With the assistance of biometrics, US-VISIT has helped stop thousands of people at POEs who were ineligible to enter the United States.

US-VISIT also supports enforcement efforts by the CBP's Office of Border Patrol to identify illegal immigrants apprehended along the borders between the POEs. Using an automated biometric system enables the rapid identification of known or suspected terrorists, criminal aliens, and repeat immigration violators, even if a person tries to conceal his or her true identity.

Did You Know?

FY 2010

When a foreign traveler provides fingerprints to a CBP officer at a POE, US-VISIT's automated systems provide identity verification and US-VISIT biometric watchlist results within 10 seconds.

U.S. Immigration and Customs Enforcement

By analyzing data regarding international travelers' entries and exits from the United States, US-VISIT identifies non-U.S. citizens who have remained in the United States beyond the amount of time for which they were admitted, known as overstays. US-VISIT's analysis includes determining whether the person is still in the United States or has left the country.

US-VISIT provides **U.S. Immigration and Customs Enforcement (ICE)** with leads on suspected overstays who are still in the United States, while those who have already left the country are added to US-VISIT's biometric watchlist to prevent re-entry.

Through the Secure Communities initiative, US-VISIT provides biometric information that enables ICE to identify criminal aliens when they are arrested by State and local law enforcement, supporting the DHS priority to identify and remove criminal aliens from the United States.

Did You Know?

FY 2010

- **US-VISIT provided a total of 30,406 overstay leads to ICE. This included additional overstay reviews previously not performed by US-VISIT, such as 11,082 overstay leads of minors and 5,923 overstay leads for previous non-priority populations.**
- **US-VISIT supported the expansion of the Secure Communities initiative to include an additional 666 jurisdictions nationwide. Adding a biometric component to the process streamlined the way ICE identifies and removes immigration violators.**
- **Nearly 263,000 aliens have been identified through the Secure Communities initiative, resulting in the removal of over 34,600 aliens from the United States.**

U.S. Department of State

US-VISIT establishes and verifies the identities of visa applicants, helping **U.S. Department of State** consular officers determine whether a non-U.S. citizen is eligible to travel to the United States.

Using biometrics and the visa application process, US-VISIT has identified thousands of people with histories of criminal or immigration violations who might otherwise go undetected.

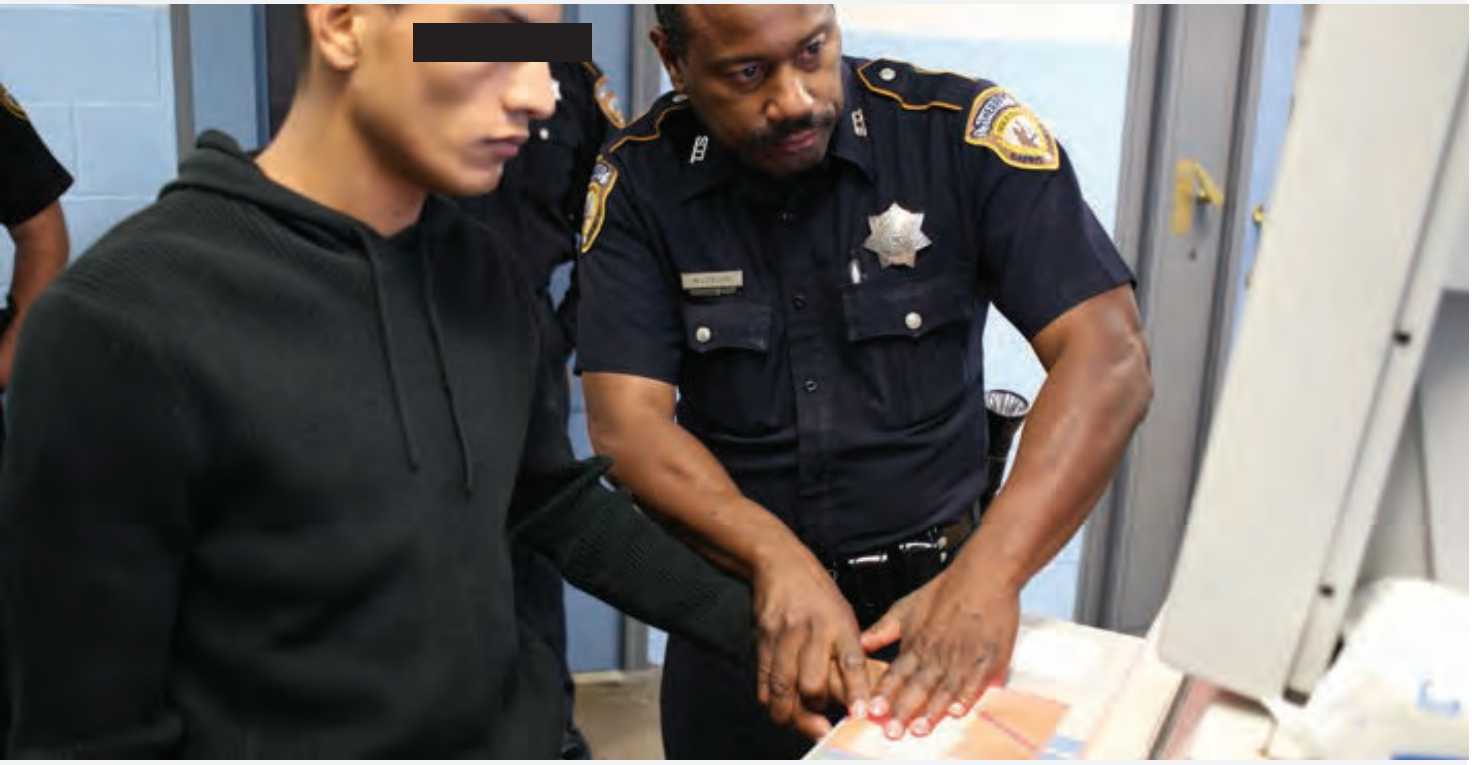
Did You Know?

FY 2010

- **US-VISIT established or verified the identities of 6.1 million applicants for visas or border crossing cards—more than 16,000 a day.**
- **US-VISIT averaged three minutes to return information to the Department of State about a visa applicant.**
- **US-VISIT's analysis of entry and exit records enabled the denial of visas or entry to more than 2,500 visa overstays attempting to return to the United States.**

U.S. Department of Justice

US-VISIT provides the **FBI** and State and local law enforcement with identifying information stored in IDENT on persons in their custody or under investigation. US-VISIT also provides details on immigration encounters to FBI special agents and to agencies working through the FBI to conduct background investigations for individuals requesting Federal Government employment, including the Office of Personnel Management and the Department of State Office of Personnel Security and Suitability.



Did You Know?

FY 2010

US-VISIT continued to enhance biometric interoperability with the FBI, and expanded data sharing with State, local, and tribal law enforcement, employment and privilege-adjudicating organizations, and international stakeholders.

U.S. Department of Defense

US-VISIT provides national security support to help the **U.S. Department of Defense (DOD)** identify known or suspected terrorists by analyzing latent biometric information collected from locations where terrorists have been. In addition, in FY 2010, US-VISIT received 90,000 fingerprint records and loaded them into IDENT.

The fingerprint records received are for known persons, as opposed to latent-print efforts. DOD has contributed a significant collection of prints to the US-VISIT biometric watchlist, including latent prints collected from improvised explosive devices and places where known or suspected terrorists have been.

Did You Know?

FY 2010

- **US-VISIT collaborated with the DOD National Ground Intelligence Center to promote known or suspected terrorists to the US-VISIT biometric watchlist to ensure that IDENT's customers have the most up-to-date information.**
- **US-VISIT standardized the business process by which it shares information with the Terrorist Screening Center to promote individuals to the US-VISIT biometric watchlist.**

Supporting Global Information Sharing

US-VISIT is involved in several global projects with foreign partners to detect and deter mala fide aliens from entering the United States or receiving immigration benefits. Since the full implementation of data sharing with the UKvisas program in September 2009, US-VISIT has shared information that aids visa screening by the United Kingdom Border Agency (UKBA) with identity matches from the US-VISIT biometric watchlist.

By collaborating with foreign governments, US-VISIT is helping to increase the number of countries that use biometrics for identity screening for border and immigration management and to expand the US-VISIT data repositories—IDENT and ADIS—with actionable biometric and biographic information. Through the expanded use of biometrics for identity-screening purposes by foreign governments around the world, US-VISIT is fostering strategic opportunities for collaboration and enabling DHS to achieve its mission of protecting our Nation from those who seek to do us harm.

US-VISIT serves as the Department's program for collecting biometrics along the travel continuum with foreign stakeholders. US-VISIT promotes the adoption of compatible standards to ensure interoperability with foreign partners and the foundation for potential biometric data sharing.

Did You Know?

FY 2010

- **US-VISIT provided information to UKvisas. At the end of FY 2010, UKBA indicated that 33 of these visa applications had been withdrawn and the applicants refused entry based on the information shared by US-VISIT.**
- **US-VISIT operationalized a biometric data exchange with Australia, Canada, New Zealand, and the United Kingdom through the High Value Data Sharing Protocol under the Five Country Conference. The protocol promotes the sharing of immigration information and asylum/refugee biometric information among the United States, Canada, Australia, and the United Kingdom.**
- **US-VISIT exchanged more than 170 records for the protocol. This number represents only individuals for whom US-VISIT has records in IDENT. As the project matures, the number of individual records could increase due to data sharing among the five countries.**
- **US-VISIT prepared for and initiated the pilot exchange of biometric prints with Germany.**

SUCCESS STORIES

US-VISIT, ICE, AND FBI TEAMS RECOGNIZED FOR WORK ON SECURE COMMUNITIES INITIATIVE

DHS, DOJ, and DOS have worked diligently in recent years to establish interoperability between the FBI's IAFIS and US-VISIT's IDENT. Collaborating with US-VISIT and the FBI's Criminal Justice Information Services (CJIS) Division, ICE's Secure Communities initiative benefits from the interoperability established between IAFIS and IDENT to quickly and accurately identify aliens in custody by local law enforcement or arrested for crimes in the United States. Together ICE, US-VISIT, and CJIS have worked to deploy this new biometric information-sharing capability to hundreds of jurisdictions nationwide.

In recognition of their innovative solutions to align these automated fingerprint identification systems, members of US-VISIT, Secure Communities, and CJIS teams were recently honored with the ICE Assistant Secretary's Protecting the Homeland Award.

US-VISIT AND FBI FINGERPRINT RECORDS TIE SUSPECTED SERIAL KILLER TO ARREST WARRANTS

In August 2010, CBP officers at Atlanta's Hartsfield-Jackson International Airport arrested a man after fingerprint records confirmed there were outstanding warrants for his arrest in connection to a murder in Michigan. The interoperability between FBI and US-VISIT systems helped CBP obtain the information they needed in a timely fashion. The man, suspected of several murders and assaults in Michigan and Virginia, was arrested as he attempted to board a flight bound for Tel Aviv, Israel. CBP officers took the man into custody and turned him over to law enforcement authorities.

US-VISIT EXAMINER'S TESTIMONY IN DRUG SMUGGLING CASE CONTRIBUTES TO GUILTY VERDICT

In June 2010, the ICE office in Phoenix, Arizona, submitted two different sets of fingerprints for two different individuals to the BSC West for comparison as part of a weapons and drug investigation. A certified 10-print examiner from the BSC determined that each set of prints matched the subject. The examiner was later subpoenaed to testify in a Phoenix trial to confirm the match of fingerprints in the case, which helped secure guilty verdicts.

US-VISIT IDENTIFIES MURDER VICTIM AND LATENT PRINT TYING SUSPECT TO THE CRIME

In March 2010, the Maricopa County, Arizona, Sheriff's Office sent the BSC fingerprints from an unknown person who had been found wrapped in a blanket after being shot and strangled to death. The BSC identified the victim after finding a match in IDENT. In April, the BSC analyzed a latent print left at the crime scene and determined it belonged to the sister of the murder suspect. The suspect's sister has been placed on the US-VISIT biometric watchlist.

US-VISIT IDENTIFIES UNITED NATIONS PERSONNEL KILLED IN HAITIAN EARTHQUAKE

After the earthquake that struck Haiti in January 2010, the Law Enforcement Liaison Officer of the U.S. Mission to the United Nations contacted the BSC for assistance in identifying deceased victims. Of the 13 sets of fingerprints submitted, the BSC identified three of the victims. The three were UN personnel who had been unaccounted for since the disaster. The BSC's identity verification enabled the UN to notify victims' families, who had waited over a month for news of their loved ones.

US-VISIT HELPS CBP IDENTIFY ILLEGAL ALIEN WITH OUTSTANDING HOMICIDE WARRANT AND CONSIDERED ARMED AND DANGEROUS

In August 2010, the Border Patrol in Yuma, Arizona apprehended a man who had entered the United States illegally. The BSC ran his fingerprints against IDENT and determined he had two outstanding warrants, including one for homicide, and was considered armed and dangerous. He was taken into custody and faces charges in the 2004 stabbing death of his girlfriend in Oregon.

US-VISIT ANALYZES LATENT FINGERPRINTS TO IDENTIFY FBI SUSPECT IN HEALTH CARE FRAUD CASE

In May 2010, the BSC identified a latent fingerprint for the FBI Cleveland Field Office related to a health care fraud case. Analysis of 34 latent prints identified the suspect as an Armenian citizen who last entered the United States in September 2009.

US-VISIT ASSISTS JOINT TERRORISM TASK FORCE BY IDENTIFYING COUNTERFEIT DOCUMENT

In November 2010, US-VISIT assisted in a case to determine the true identity and overstay status of a Turkish man attempting to gain employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity to prove his legal status to reside and work in the United States. The subject was subsequently arrested by local DHS law enforcement authorities as an overstay and placed into Federal custody awaiting removal proceedings.

MOVING FORWARD
2011 GOALS

In FY 2011, US-VISIT will continue to improve its technology and services to be more efficient, accurate, and effective. It will also continue collaboration on biometric initiatives with other nations.

MEETING DHS DATA CONSOLIDATION DIRECTIVES

The Data Center Mirroring and Migration initiative will continue to progress toward the DHS data center consolidation goal by relocating US-VISIT systems and hosting services from the DOJ data centers to the two DHS data centers in FY 2011. When this initiative is completed in FY 2012, US-VISIT will have mirrored systems at the two DHS data centers, with redundant capabilities in the event of a system outage or a hardware failure. The project will support a high level of disaster recovery and availability for US-VISIT applications.

ENHANCING IDENT/IAFIS/ABIS INTEROPERABILITY

In FY 2011, US-VISIT will finalize, design, build, and begin testing the interface between IDENT and DOD's Automated Biometric Identification System (ABIS). This will permit communication between the two systems, allow each system to be searched for matches to stored biometric data, and enable the search results to be returned. A related effort will develop requirements for an automated capability to share latent prints for search results.

US-VISIT will also initiate a record-linking design to allow for the subsequent retrieval of information on an individual already "linked" in other biometric databases, minimizing the number of identification searches and improving operational efficiencies and response times.

ADVANCING US-VISIT 1.0

In FY 2011, US-VISIT will continue planning for the US-VISIT 1.0 initiative. The objective of the US-VIST 1.0 investment is to address gaps in availability, flexibility, scalability, and affordability posed by US-VISIT's two major automated identification systems—IDENT and ADIS—in support of its mission. The US-VISIT 1.0 initiative will leverage new tools, technologies, and approaches to integrate US-VISIT's biometric and biographic applications into a comprehensive set of automated services that will meet and exceed operational requirements well into the future, while reducing the overall cost per transaction.

CONTINUING INTERNATIONAL COLLABORATION

In FY 2011, US-VISIT will continue to build on the program's success by creating and maintaining strategic coalitions with international partners as countries around the world recognize the power of biometric technology in their immigration and border management systems.

US-VISIT will work to increase commonality in biometric standards and best practices, develop protocols for sharing critical information, provide technical assistance to countries implementing biometrics, and jointly test and deploy innovative biometric techniques.

Cooperation, collaboration, and appropriate information sharing are essential to achieving global security. Expanding international partnerships will create a robust and resilient 21st century immigration and border management system.

US-VISIT will provide biometric intelligence reporting to DHS and the intelligence and law enforcement communities. And US-VISIT will continue to provide research and coordination for all international and domestic programs that impact the US-VISIT biometric watchlist.

SUPPORTING THE INTELLIGENCE COMMUNITY

In FY 2011, US-VISIT will continue to provide research and coordination for all international and domestic programs that impact the US-VISIT biometric watchlist. By the end of the fiscal year, US-VISIT will be able to provide biometric intelligence reporting to DHS and the intelligence and law enforcement communities, while increasing US-VISIT biometric watchlist reviews and adjudications by 25 percent over FY 2010 levels.

US-VISIT will also continue to maintain full-time operational support at FY 2010 levels. This will consist of analysts capable of researching biometrically verified hits against IDENT data submitted by the FBI, DHS entities, security offices maintaining access control to critical infrastructure facilities, and other contributing agencies to leverage biometric and biographic capabilities.

Homeland Security

US-VISIT

Web Site:
For more information, visit the US-VISIT program Web site at www.dhs.gov/us-visit.

Privacy Policy:
US-VISIT upholds the privacy of individuals while helping protect our national borders and immigration system. Personal information collected by US-VISIT will be used only for the purposes for which it was collected, unless specifically authorized or mandated by law. Questions or concerns relating to personal information and the US-VISIT program may be directed to the US-VISIT Privacy Officer, US-VISIT program, Department of Homeland Security, Washington, D.C. 20528, or usvisitprivacy@dhs.gov.