John H. Marburger III

Science Advisor to the President
Director, Office of Science and Technology Policy

September 12, 2007

Taking Today's Biometrics to Meet Tomorrow's Needs

Biometrics & Identity Management

Duane Blackburn
Office of Science & Technology Policy

September 12, 2007

Recent BCC History

- 2001 (cancelled due to 9/11)
  - Single Track
  - No discussion of USG operational biometric programs
  - Three casual mentions of projects that involve multiple agencies
- 2004
  - Is Biometrics a Science?
  - *The Structure of Scientific Revolutions*, Thomas Kuhn
  - Biometrics Paradigm
- 2006
  - *The National Biometrics Challenge*
  - Biometrics as a foundation for solving identity problems
- 2007
  - Three tracks
  - Discussion of multiple USG operational biometric programs
  - Interagency collaboration is modus operandi
  - "Identity Management"

Biometrics.gov

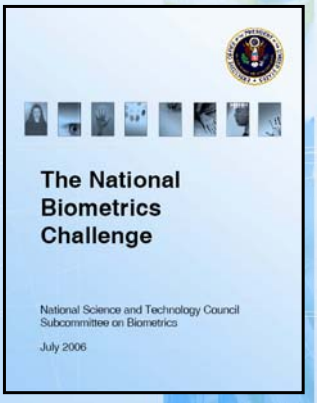
What is Identity Management in the 21st Century?

- We are still in early stages of that discussion
- Four items can provide a starting point within the USG:
  - The National Biometrics Challenge
  - Defense Science Board Task Force on Biometrics
  - Quick-look of programs with PII
  - Identity Concentricity Model

Biometrics.gov

The National Biometrics Challenge

- Identity Management:
  - The combination of systems, rules and procedures that defines an agreement between an individual and organization(s) regarding ownership, utilization and safeguard of personal identity information
- Identity Governance
  - The combination of policies and actions taken to ensure enterprise-wide consistency, privacy protection and appropriate interoperability between individual identity management systems.



http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf

Biometrics.gov

Defense Science Board TF on Biometrics

- "Identity Management is a set of processes, policies, tools, connectivities, and social contracts protecting the creation, maintenance, use and termination of a digital identity."
- "An identity management system…is meant to include both algorithms – their instantiation in software/hardware – as well as data. The data are an organized collection of information about specific individuals"
- "There can be no truly accurate Identity Management system without biometrics."
  - In order to achieve, verify and sustain that root identity, it is absolutely necessary to link the legend to the person making the claims.

Note: This will be briefed on Thursday.
www.acq.osd.mil/dsb/reports/2007-03-Biometrics.pdf

Biometrics.gov

Quick-look of Programs with PII

- Objective
  - Perform a fast, initial, analysis of federal programs that involve personally identifiable information (PII)
- Questions
  - How many are there?
  - Can we *start* to understand how they are similar and where they diverge?
  - Can we *start* to develop any general observations?
- Approach
  - Extreme ADD analysis of Privacy Impact Assessments
    - 10 second review of all to place in bins
    - Select a few from each bin to review in more depth

Biometrics.gov

Analysis Limitations

- Very fast, very high-level, analysis
- Restricting analysis to PIAs limits information available
  - PIAs vary in specificity
  - Effectiveness and true cost of IdM components difficult to ascertain
    - Effectiveness is the ability to correctly manage identity
  - Difficult to determine dependencies and interdependencies that are critical to success

You wouldn't want to base decisions on this analysis, but it serves as an interesting first step!

Biometrics.gov

Initial Observations

- Large number of programs (>1500) within the federal government have an IdM component
  - Diversity in scale, scope, and application
  - Most of these programs have IdM as a means to an end and are not used to manage only an identity
- Identity management implementation appears to be principally program oriented
  - Initial analysis did not reveal a common foundation for definitions, processes, metrics or security
  - Different agencies appear to use different procedures to manage identity throughout the system lifecycle
- Program discussion appears to focus on the here & now

Biometrics.gov

Potential Implications

If initial observations prove true:

- Different procedures for IdM could inhibit data sharing
  - To detect duplication, fraud, misuse
  - Could miss identifying someone
  - Could misidentify someone
  - Loss of cost sharing benefit
- Negative impact on privacy protections
- Cross-function analysis would be inhibited
  - Difficult to understand/compare/mitigate risks and impacts within or across enterprises
  - Difficult to establish expectations and requirements independently of organization
  - Can't determine prioritization of IdM program restoration during a crisis
  - Can't determine which programs should serve as a model of efficiency (or security, privacy protection, etc.) or which are exemplars of how to manage identity incorrectly

Biometrics.gov

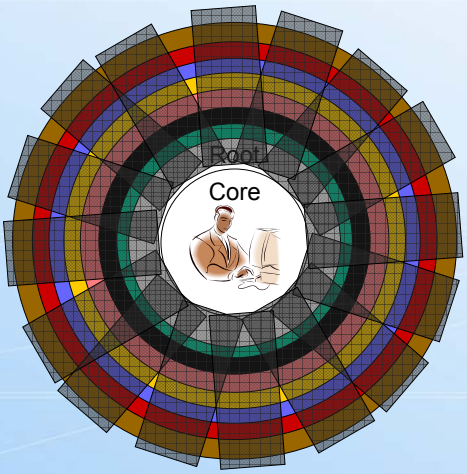
So, is all that bad?

No! "Digital" IdM science is in its infancy

- Forcing programs to merge into standard formats in early adoption stages stifles innovation, which inhibits operational capabilities (including privacy protection)
- However, we may now be at the point where setting standards and policies is now required to advance IdM science further
  - Some work is already starting
- Next Step – more detailed analysis

Biometrics.gov

Identity Concentricity



Application 1
Enrollment
Usage

Application 2
Enrollment
Usage

Application 3
Enrollment
Usage

Application 4
Enrollment
Usage

Application 5
Enrollment
Usage

Application 6
Enrollment
Usage

Application 7
Enrollment?

Biometrics.gov

Meta-analysis

- This stuff is complicated!
  - Potentially makes biometric issues look *easy*
  - It is more than simply a technology issue
  - Multiple IdM constituencies, standards, experts, etc., makes this even more complicated
- The front and back ends are both important
- Biometrics will play a key role in IdM systems that require a close association with the individual
- There are many IdM applications already
  - Which may or may not understand their reliance and impact on others
- It's time to shape IdM on the whole

Biometrics.gov

IdM Building Blocks

- HSPD-12; PIV
  - Multiple groups with varying interests worked together to develop an approach that is generally agreeable
  - Significant back-end infrastructure in place to establish a trusted root identity
  - Large scale implementation
  - Foundation is being leveraged for other public & private sector programs
- Federal Biometric Efforts
  - Biometrics are closest real-time association with a core identity possible
  - Federal system of systems enables "one person, one identity" when necessary

Biometrics.gov

NSTC Subcommittee on Biometrics and Identity Management

- National Science & Technology Council
  - Cabinet-level Council is the principal means within the executive branch to coordinate S&T policy across the diverse entities that make up the Federal R&D enterprise.
  - Established by Executive Order 12881
- Subcommittee on Biometrics
  - Develop and implement multi-agency investment strategies that advance biometric sciences to meet public and private needs;
  - Coordinate biometrics-related activities that are of interagency importance;
  - Facilitate the inclusions of privacy-protecting principles in biometric system design;
  - Ensure consistent message about biometrics and government initiatives when agencies interact with Congress, the press and the public;
  - Strengthen international and public sector partnerships to foster the advancement of biometric technologies.
- "and Identity Management" added in spring of 2007

Biometrics.gov

Subcommittee Growth

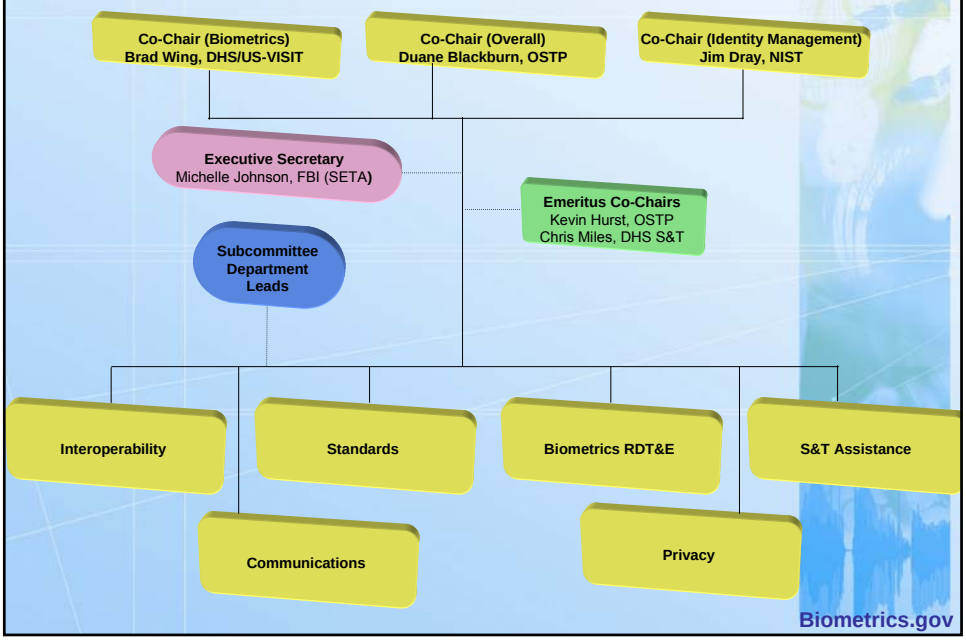
Phase I – Forming 2002-2003	Phase 2 - Storming 2003-2006	Phase 3 - Norming 2006-Present
Goals: • Share lessons learned from operational systems • Grow USG biometrics expertise • Build relationships	**Goals:** • Advance technology, privacy & communications • Grow USG biometrics expertise • Build relationships	**Goals:** • USG-wide biometric system of systems • Community able to meet other government and private sector needs • Accurate national discussions
Deliverables • List of topics for potential collaboration • Initiate joint RDT&E efforts • No fisticuffs!	**Deliverables** • Joint RDT&E topics • Foundational documents • Privacy paper & websites • *The National Biometrics Challenge*	**Deliverables** • System of Systems framework • USG-wide plans for standards, RDT&E, privacy & communications • Enhanced operational capabilities

Example Successes of the Subcommittee

- Documents
  - "Biometrics Foundation" Suite
  - *Privacy & Biometrics – Building a Conceptual Foundation*
  - *The National Biometrics Challenge*
  - Website Suite
    - www.biometrics.gov, www.biometricscatalog.org and www.biometrics.org
      - www.biometria.gov.ar
- Technical Examples
  - Fast Fingerprint Capture RFI
  - Rolled Fingerprint Equivalent Research
  - FRVT, FRGC, FpVTE, ICE
  - Coordination of USG in Standards Bodies
  - International Privacy Workshops
- Unmeasurables
  - Today's oft-discussed USG biometric systems (HSPD-12, TWIC, FBI's NGI, etc.) rely heavily on the prior work of the subcommittee
  - Increased USG knowledge of biometrics
  - Developed relationships & comfort working cross-agency
  - Better public perception of USG biometric activities
  - Better recognition of biometric initiatives & needs by upper management

Biometrics.gov

Subcommittee Organizational Framework



Biometrics.gov

Activity Areas

- Interoperability (Kim Del Greco, FBI)
  - USG-wide biometric system of systems governance/coordination
    - Build upon solid foundation of biometric systems in major USG agencies
    - Promote adoption of multi-modal biometric capabilities
    - Streamline watch list data availability/usability/control
    - Make recommendations on how best to accommodate extended interoperability requirements
- Standards (Mike Hogan, NIST; Brad Wing, US-VISIT)
  - Support interoperability requirements & needs of biometric community
    - Standards Development
    - Conformity Assessment
    - USG Adoption

Biometrics.gov

Activity Areas (continued)

- Biometrics RDT&E Coordination (Chris Miles, DHS S&T; Tom Dee, DoD)
  - Develop and implement a multi-year, USG-wide, biometrics RDT&E agenda
  - Liaison between NSTC/Biometrics and public sector
    - *The National Biometrics Challenge*
- Biometrics S&T Guidance/Assistance (Bill Baron, DOT VOLPE Center)
  - Quick response team to answer technical questions from senior level feds on biometric issues
  - Bring operational issues/concerns into technology area activities
  - Update foundation docs

Biometrics.gov

Activity Areas (continued)

- Communications (Kim Weissman, US-VISIT)
  - Outreach & messaging support
  - Maintenance of USG Biometric Websites
  - Other activities (press outreach, etc.)
- Privacy (Peter Sand, DHS Privacy Office; Niels Quist, DOJ Privacy and Civil Liberties)
  - Develop reference material to further the community's understanding of the nexus of biometric technologies and privacy theory
  - Develop USG policies & procedures, and associated training material so that privacy is fully integrated into USG system planning

Moving Forward

- Remainder of this session
  - Additional details on
    - Interoperability
    - Standards
    - RDT&E
    - Privacy
  - Q&A
- Post-Conference
  - Partnering with private sector, foreign governments
  - Information exchange is critical
  - Keep working to meet the Challenge

Duane Blackburn
dblackburn@ostp.eop.gov
202-456-6068

Biometrics.gov

Driving Federal Biometric Interoperability

Kim Del Greco
FBI Criminal Justice Information Services Division

September 12, 2007

Interoperability

- Definition
  - IEEE defines interoperability as: “the ability of two or more systems or components to exchange information and to use the information that has been exchanged.”
- Challenges
  - Policy Issues
  - Technological Hurdles
  - Agency Business Objectives

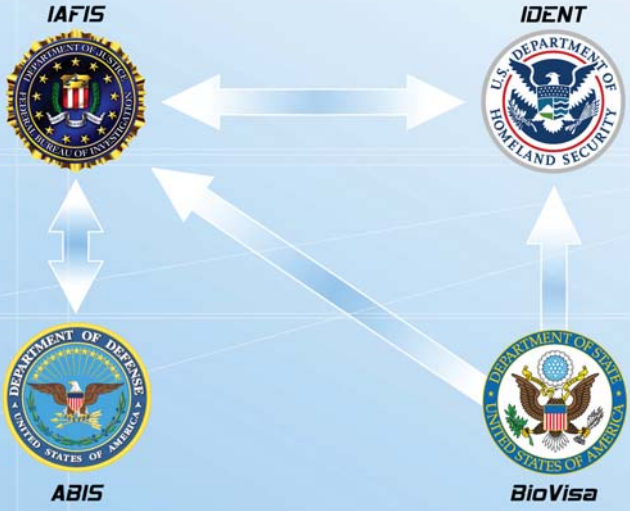
Biometrics.gov

Historic Perspective

- Pre 9/11
  - Legal/procedural restrictions separated intelligence and criminal investigations
  - Need for information sharing and interoperability not emphasized
- Policy Drivers For Interoperability
  - Homeland Security Information Act of 2002
  - USA PATRIOT Act (Oct. 2001)
  - U.S. Attorney General Directive (Apr. 2002)
  - Presidential Executive Order 13388 (Oct. 2005)
  - Homeland Security Presidential Directive-12 (Aug. 2004)

Biometrics.gov

Where Are We Today?



Success Stories

- iDSM (IAFIS/IDENT)
  - Hit "#214" August 22, 2007 – Dallas County, TX
    - IAFIS data uncovered: DWI, Alien Inadmissibility, and three different name changes
    - DHS/ICE action taken: Suspect detained and further investigated, revealing a murder charge
  - Mohamad al Khatani – purported 20th hijacker in 9/11 terrorist attacks
    - Identified through DHS immigration record from August 2001
    - Matched and hit against IAFIS most-wanted terrorists list in December 2001

Biometrics.gov

Success Stories (cont.)

- IAFIS/INTERPOL Red Notices
  - Aug. 2007 - USCIS applicant produced hit against IAFIS/INTERPOL Red Notices database
  - DHS action taken: Suspect detained and further investigated, revealing a murder charge
- DoD ABIS/FBI IAFIS - Quick Capture Platform
  - FBI Hostage Rescue Team receives:
    - 54M IAFIS Criminal Master File and DoD ABIS
    - Full search in less than 2 minutes while in theatre (Afghanistan and Iraq)
- DoS/IAFIS
  - June 2007 – El Salvador Consulate Office
  - False name given
  - Ten-Print Pilot: IAFIS record revealed previous deportation, leading to arrest

Road Ahead

- United States government (USG)-wide biometric system of systems governance/coordination
  - Build upon solid foundation of biometric systems in major USG agencies
  - Promote adoption of multimodal biometric capabilities
  - Streamline watch list data availability/ usability/control
  - Make recommendations on how best to accommodate extended interoperability requirements

Taking Today's Biometrics to Meet Tomorrow's Needs

Standards

Michael D. Hogan
Co-Chair, Standards & Conformity Assessment Working Group (SCA WG)
NSTC Subcommittee on Biometrics & Identity Management

September 12, 2007

Meeting the Challenge: Progress and Participation

- In August 2006, the *National Biometrics Challenge* identified four major challenges.
- One was to establish standards for plug-and-play performance and biometric systems interoperability.
- In response, the Standards & Conformity Assessment Working Group (SCA WG) of the National Science and Technology Council (NSTC) Subcommittee on Biometrics & Identity Management has developed a framework to reach interagency consensus on biometric standards adoption for the Federal government, approved as policy by the NSTC Committee on Technology.
- This presentation reviews this policy and the ongoing USG planning to implement this policy in support of biometric data exchange and interoperability across USG agencies.

Biometrics.gov

Ongoing Work

- **Policy Document**
- **Registry of Biometric Standards**
  - The Subcommittee will analyze standards and develop consensus on which should be adopted.
- **Action Plan**
  - Describes the actions the Subcommittee and agencies will take to implement the approved policy.
- **Supplemental Information**
  - Provides background information on standards, SDOs, etc.
- As approved, these documents will be posted at
  - standards.gov/biometrics and biometrics.gov/standards

Biometrics.gov

Status of NSTC Policy

- The NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards was approved on September 8, 2007.
- In this policy document, the NSTC Subcommittee on Biometrics and Identity Management is often referred to as "the Subcommittee."

Biometrics.gov

Principles and Key Actions

- *Continued development of voluntary consensus standards for biometrics is vital to the security of our Nation and the stability of the US-based biometrics community.*
  - Agencies should support national and international voluntary biometric standards development activities.
- *Rigorous testing is required to ensure vendor and system compliance with biometric standards*.
  - Agencies should support the development of harmonized conformance, interoperability, performance, security, human factors, and operational scenario testing programs in support of procurement actions for biometric products, programs and services.
- *Standards and conformity assessment processes must be identified and adopted across all agencies to ensure full interoperability.*
  - Agencies should participate in an interagency process led by the Subcommittee to review available standards and develop consensus recommendations regarding which standards should be uniformly adopted across the USG.

Biometrics.gov

Principles and Key Actions

- *The biometric standards and conformity assessment processes recommended by the Subcommittee should be promulgated*.
  - The Subcommittee should develop a registry of adopted biometric standards at www.standards.gov/biometrics.
- *The biometric standards and conformity assessment processes recommended by the Subcommittee should be integrated into agency plans whenever feasible*.
  - Agencies should strive to build and operate biometric systems that are based on the Subcommittee's recommended standards.
- *Timely adoption and use of appropriate standards is critical to achieving biometrics goals*.
  - Following selection of recommended standards, the Subcommittee should work to advance adoption of standards for use in Federal biometrics programs and services.

Biometrics.gov

Implementation Tasks

- The following are the initial and ongoing tasks necessary for the implementation of this policy.
- The Subcommittee is directed to further develop these tasks into a comprehensive interagency action plan.

Biometrics.gov

Implementation Tasks

USG Participation in Biometric Standards Development

- USG agencies should continue to provide administrative and technical leadership for national and international biometric standards development, and should coordinate USG positions and contributions to these standards developers through the Subcommittee.
- Based upon each agency's mission, USG agencies should participate in relevant biometrics and related standards developing organizations (SDO).

Biometrics.gov

Implementation Tasks

Backwards Compatibility of Standards

- While participating in SDO activities, the USG should promote the concept that voluntary consensus standards be backward compatible to the maximum extent possible to ensure interoperability of new systems with legacy data, or new data with legacy systems.

Biometrics.gov

Implementation Tasks

Interagency Analysis and Determination of Recommended Standards for USG Adoption

- The NSTC Subcommittee on Biometrics and Identity Management should establish definitions for emerging, mature, and stable biometric standards.
- Based upon these model criteria, the Subcommittee should review available standards and collectively determine and promulgate which standards should be recommended for adoption throughout the USG.

Biometrics.gov

Implementation Tasks

Consistent Application of Biometric Standards in Agency Plans

- The NSTC Subcommittee on Biometrics and Identity Management should assist agencies as they develop biometric system plans to ensure that recommended standards and associated testing are used to the maximum extent practicable
- Agencies should develop internal procedures to ensure citation of relevant standards from the registry of USG recommended biometric standards in biometric procurement actions.

Biometrics.gov

Implementation Tasks

Exchange of Proprietary Data

- Agencies should use the proprietary data fields in standardized data formats from the registry of USG recommended biometric standards for the exchange of proprietary data.
- Agencies with closed systems that do not require system or interagency interoperability should only use proprietary data formats if standardized data formats can be documented to be inadequate.

Biometrics.gov

Implementation Tasks

Lifecycle Handling of Biometric Samples

- The NSTC Subcommittee on Biometrics and Identity Management should develop a set of guidelines to ensure the quality and usability of biometric samples.
- This guidance should highlight the importance of obtaining raw biometric samples upon collection (using biometric standards on the registry of USG recommended biometric standards when possible) and deprecate the collection of biometric templates only.

Biometrics.gov

Implementation Tasks

Consistent Collection and Use of Metadata

- The NSTC Subcommittee on Biometrics and Identity Management should support agencies as they develop agency-specific guidelines for the collection, maintenance, and use of metadata for USG biometric applications.

Biometrics.gov

Roles and Responsibilities

- This policy requires multiple interagency actions as well as departmental actions to ensure successful implementation.
- The NSTC Subcommittee on Biometrics and Identity Management is the responsible party for developing interagency consensus and facilitating agency adoption in support of this policy.
- By participating actively in the Subcommittee, agencies are ensured that their requirements will be considered in the interagency review and determination of which standards should be adopted.

Biometrics.gov

Roles and Responsibilities

The NSTC Subcommittee on Biometrics and Identity Management is the responsible party for the:

- Coordination of USG activities in national and international voluntary biometric standards development;
- Establishment of model criteria for the adoption and maintenance of biometric standards;
- Interagency analysis, determination and promulgation of recommended standards for USG adoption;
- Facilitation of access to adopted standards by USG personnel; and
- Identification of research, development, test and evaluation needs that are required to enable this Policy, and prioritization of those needs in the Subcommittee's ongoing RDT&E agenda development.

Biometrics.gov

Roles and Responsibilities

The roles and responsibilities of agencies with biometric programs are to:

- Support the Subcommittee's designated responsibilities by ensuring appropriate agency personnel and resources are provided;
- Ensure the use of appropriate biometric standards from the registry of USG recommended biometric standards internally and in awarded projects, unless the standards can be documented to be operationally inadequate or are fiscally untenable for the anticipated benefits;
- Identify agency-specific requirements on the use of biometric standards (capture, use, dissemination, and disposition of biometric data) consistent with *The National Biometrics Challenge*; and
- Ensure compliance, where applicable, with the requirements of the Privacy Act of 1974 and the E-Government Act of 2002 when using standards-based biometric image or template data, as it is considered to be personally identifiable information.

Biometrics.gov

Michael D. Hogan
m.hogan@nist.gov
301-975-2926

Taking Today's Biometrics to Meet Tomorrow's Needs

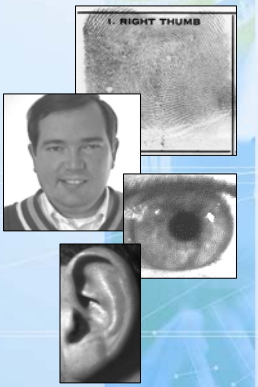
Technology Activities of the NSTC Subcommittee on Biometrics and Identity Management

Chris Miles
DHS/S&T/HFD

September 12, 2007

Advancing Technology

- NSTC Subcommittee on Biometrics works cooperatively to advance:
  - Fingerprint Recognition
  - Face Recognition
  - Iris Recognition
  - Next Generation Biometrics
  - Multi-Biometrics
  - Test and Evaluation of Biometrics



FACE RECOGNITION VENDOR TEST

FRGC
FACE RECOGNITION GRAND CHALLENGE

ICE
IRIS CHALLENGE EVALUATION

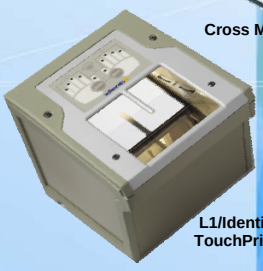
Biometrics.gov

Technology Successes

Fast 10-print Slap Capture of Fingerprints

- Joint Federal government user group issued an industry challenge via RFI in Sep. 2005
- The Challenge called for industry to provide:
  - 10-print flat capture devices and software
  - < 6 inch x 6 inch x 6 inch size
  - < 5 lbs. weight
  - < 15 seconds capture time
- CrossMatch announced LScan Guardian in April, 2006
- Identix announced TouchPrint(TM) Enhanced Definition 4100 Slap & Roll Live Scan in June, 200
- Other product announcements have followed this year

Cross Match Guardian



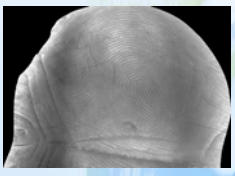
L1/Identix TouchPrint

Biometrics.gov

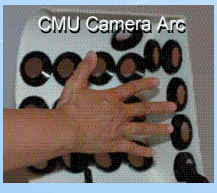
Technology Successes

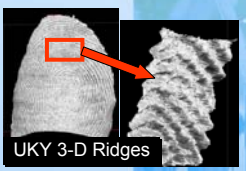
Fast Rolled-Equivalent Fingerprints

- Highly cooperative, joint effort of DOJ, DHS, DoD, and State
- A major step forward in finger and palm print capture technology:
  - Capture of 10 rolled-equivalent fingerprints in <15 seconds
  - Capture of both palms in 1 minute or less
- Four R&D efforts underway to produce prototype devices in 18 months to 2 years.



TBS Prototype
10 finger Capture Device
delivered to NIJ in June 2007



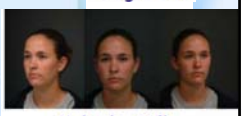


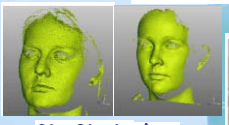
Biometrics.gov

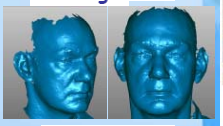
Technology Successes

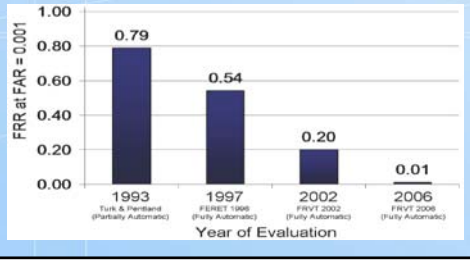
Face Recognition Vendor Test 2006

- Achieved FRGC goal of improving performance by an order of magnitude over FRVT 2002.
- Established the first 3D face recognition bench-mark.
- Showed significant progress has been made in matching faces across changes in lighting.
- Showed that face recognition algorithms are capable of performing better than humans.
- Executed by NIST. Sponsored by many USG partners







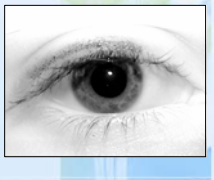


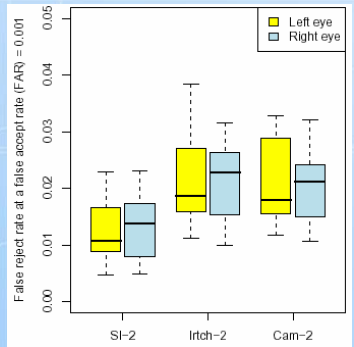
Biometrics.gov

Technology Successes

Iris Challenge Evaluation (ICE 2006)

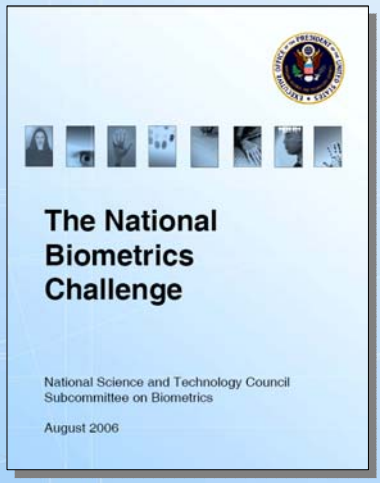
- ICE 2005 was a challenge problem and had 9 participating organizations and 15 algorithms submitted
- ICE 2006 is an independent evaluation and had 3 participants
- Executed by NIST. Sponsored by many USG partners





Biometrics.gov

The National Biometrics Challenge



- Released in August 2006
- Identifies common challenges to providing robust identity tools and deploying those tools to meet real-world needs
- Provides an analysis of:
  - Unique attributes of biometrics
  - Market forces and societal issues
  - Advances required for next-generation capabilities
  - Communications and Privacy
  - Government's Role in Biometrics

Biometrics.gov

Outstanding Technology Needs

Primary Driving Forces

5.1 Biometric Sensor Challenges

Biometrics Challenges	National Security	Law Enforce.	Homeland Security &	e-Gov Services	Enterprise & Business Trans.	Information & Personal
Rapid collection in mobile and harsh environments enabling immediate submission to national level screening	x	x				
Quality collection of non-cooperative persons at distances	x	x				
Quality collection in relaxed conditions	x	x				
Templates that can revoked/replaced if compromised	x	x		x	x	
Next Generation Sensors	x	x		x	x	

Anticipated Benefits:

- Rapid collection in uncontrolled situations for accurate, rapid, safe and easy comparison and addition to national-level screening systems
- Real-time comparison of first-time foreign visitors to terrorist/criminal databases
- Single identity of individuals across law enforcement enterprise (field, police station, court, jail, etc.)
- Fiscal viability in enterprise-security and financial transactions
- System capabilities unaffected by changes in sensors
- Templates that protect against identity theft without degrading system performance

Biometrics.gov

Outstanding Technology Needs

Focus for Research to Accomplish 5.1 Biometric Sensor Challenges:

- Sensors that automatically recognize the operating environment and communicate with other system components to automatically adjust settings to deliver optimal data
- Virtually no failures-to-enroll
- Low cost
- Easy to use (intuitive to end-users)
- Standards-based data output
- Easily integrated into existing systems
- Incorporate liveness detection
- Rugged (varying operating temperatures, waterproof and UV-resistant)
- Collect standards-quality imagery from a distance
- Fingerprint Sensors that provide:
  - Rapid and intuitive collection (less than 15 seconds) of rolled- equivalent fingerprints from cooperative users
  - Contactless and/or self-sterilizing contact fingerprint sensors
- Middleware techniques/standards that will permit biometric sensor "plug-and-play" capability
- Conformance testing suites/programs for data quality and middleware standards
- Scenario and performance testing to assure that equipment will meet intended performance metrics for specific applications
- Transformed revocable and replaceable biometric templates created at time of capture

Biometrics.gov

Outstanding Technology Needs

Primary Driving Forces

5.2 Biometric System Challenges

Biometrics Challenges

	National Security	Law Enforce.	Homeland Security &	e-Gov Services	Enterprise & Business Trans.	Information &	Personal
Consistently high recognition accuracy under a variety of operational environments	x		x	x	x	x	
Ability to determine which components are most appropriate for a given application	x		x	x	x	x	
Intuitive interfaces for operators and end-users	x		x	x	x	x	
Remote, unattended enrollment and recognition of end-users with varying sensors					x	x	
Return on investment models for various applications to aide in determining the efficacy of incorporating biometrics	x		x	x	x	x	

Anticipated Benefits:

- Ability to use biometrics systems regardless of the operational environment
- Increased likelihood of problem-free, successful installations of biometrics systems
- Reduced reliance on individual vendors
- Viability of large-scale use of biometrics in electronic transactions for reducing identity theft potential
- User confidence in biometrics system performance

Biometrics.gov

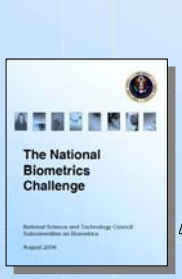
Outstanding Technology Needs

Focus for Research to Accomplish 5.2 Biometric System Challenges:

- Enhanced matching algorithms
- Standard sensor-system communications to ensure collection of usable data
- Uniform data quality measures
- Integration of multiple sensors, matching algorithms and modalities in a single system
- Automated assessment of which modalities and sensors should be used in a given operational environment
- Publicly available evaluation results on sensors and matching algorithms
- Analysis of end-user interfaces to biometrics systems followed by development of guidelines for future adoption
- Quality measures and standards to assist decision making in the matching process
- Standards for interoperability of biometric templates, conformance testing of products that purportedly meet the standard and analysis/revision of the standard as needed
- Development of biometrics ROI models for common applications within the driving forces
- Analysis of the scalability of biometrics systems, followed by research on scalability improvements

Biometrics.gov

Coordinated RDT&E Agenda



Biometrics Industry Feedback

Biometrics Academia Feedback

Inter-Operability Plan

RDT&E Group

	FY09	FY10	FY11	FY12	FY13
5.1 Biometric Sensor Challenges					
5.2 Biometric System Challenges					
5.3 Biometric System Interoperability					
5.4 Communications and Privacy					

Biometrics.gov

Privacy & Biometrics

NSTC Subcommittee
Biometrics & Identity Management
Privacy working group

Peter E. Sand, JD, CIPP/G
Director of Privacy Technology
U.S. Department of Homeland Security

September 12, 2007

Overview

- What is Privacy & Biometrics
- Fair Information Practice Principles
- Privacy Compliance Life Cycle
- Privacy Technology Guide
- Where to start: Pragmatic First Steps

Biometrics.gov

What is Privacy & Biometrics

- National Biometrics Challenge
  - "Fundamental understanding of... privacy principles."
  - "Embed privacy functionality into every layer of the architecture."
  - "Privacy-protective solutions that meet operational needs...."
- Implementation: Integrate throughout Subcommittee efforts – all levels/projects
- Biometric data = PII
- Focus: government operations
  - Principles
  - Process: Compliance life cycle

Biometrics.gov

Fair Information Practice Principles (FIPPs)

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

Guiding Principles - applied pragmatically

Biometrics.gov

Fair Information Practice Principles (FIPPs)

Transparency
: Be transparent and provide notice to the individual regarding the collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in applicable privacy compliance documentation. There should be no system the existence of which is a secret.

Individual Participation
: Involve the individual in the process of using PII. To the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and provide mechanisms for appropriate access, correction, and redress regarding use of PII.

Purpose Specification
: Specifically articulate the authority which permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.

Data Minimization
: Only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with records disposition schedules.

Biometrics.gov

Fair Information Practice Principles (FIPPs)

Use Limitation
: Use PII solely for the purpose(s) specified in the notice. Sharing PII outside the agency should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity
: To the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Security
: Protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing
: Be accountable for complying with these principles, providing training to all employees and contractors who use PII, and audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Biometrics.gov

Privacy Compliance Life Cycle

1. Initial Contact and Coordination
2. Collaboration and Development
3. Reporting
4. Auditing

Biometrics.gov

Privacy Compliance Life Cycle

Initial Contact and Coordination

- Identify the project and determine the applicable level of required analysis and documentation.
- A short assessment form should document the results of this stage.

Collaboration and Development

- Integrate the applicable analysis and documentation into development to ensure that privacy protections are included in the set of business requirements and the design and deployment.
- A longer assessment form and applicable legal documents should document the results of this stage.

Biometrics.gov

Privacy Compliance Life Cycle

Reporting

- Report on the status of privacy compliance analysis and documentation related to each project and the overall inventory.
- Standardized enterprise level reviews should document the results of this stage.

Auditing

- Analyze the project's incorporation and performance of all applicable privacy compliance requirements.
- Specific audit reports should document the results of this stage.

Biometrics.gov

Privacy Technology Implementation Guide (PTIG)

Privacy protections - Contextualized

- Management
  - Identify full scope
  - Structured processes
  - Alignment
- Development
  - Dictionaries & Models
  - Data Quality Standards
  - System Logs

Biometrics.gov

Pragmatic First Steps

- Coordinate with your Privacy Office
- Describe full biometric SYSTEM
- Full scope: Data & Use life cycles
- Define procedural requirements
  - Analyze & Document
  - Risks and mitigations
- Build protections into systems
- Value across all sectors: Add privacy into proposals/responses to show awareness & solutions

Biometrics.gov