National Science and Technology Council

Subcommittee on Biometrics and Identity Management

Duane Blackburn
Office of Science and Technology Policy
Executive Office of the President

September 24, 2008

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Subcommittee Growth

Phase I

2002-2003

Goals:

- Share lessons learned from operational systems
- Grow USG biometrics expertise
- Build relationships

Deliverables

- List of topics for potential collaboration
- Initiate joint RDT&E efforts

Phase 2

2003-2006

Goals:

- Advance technology, privacy & communications
- Grow USG biometrics expertise
- Build relationships

Deliverables

- Joint RDT&E topics
- Foundational documents
- Privacy paper & websites
- *The National Biometrics Challenge*

Phase 3

2006-Present

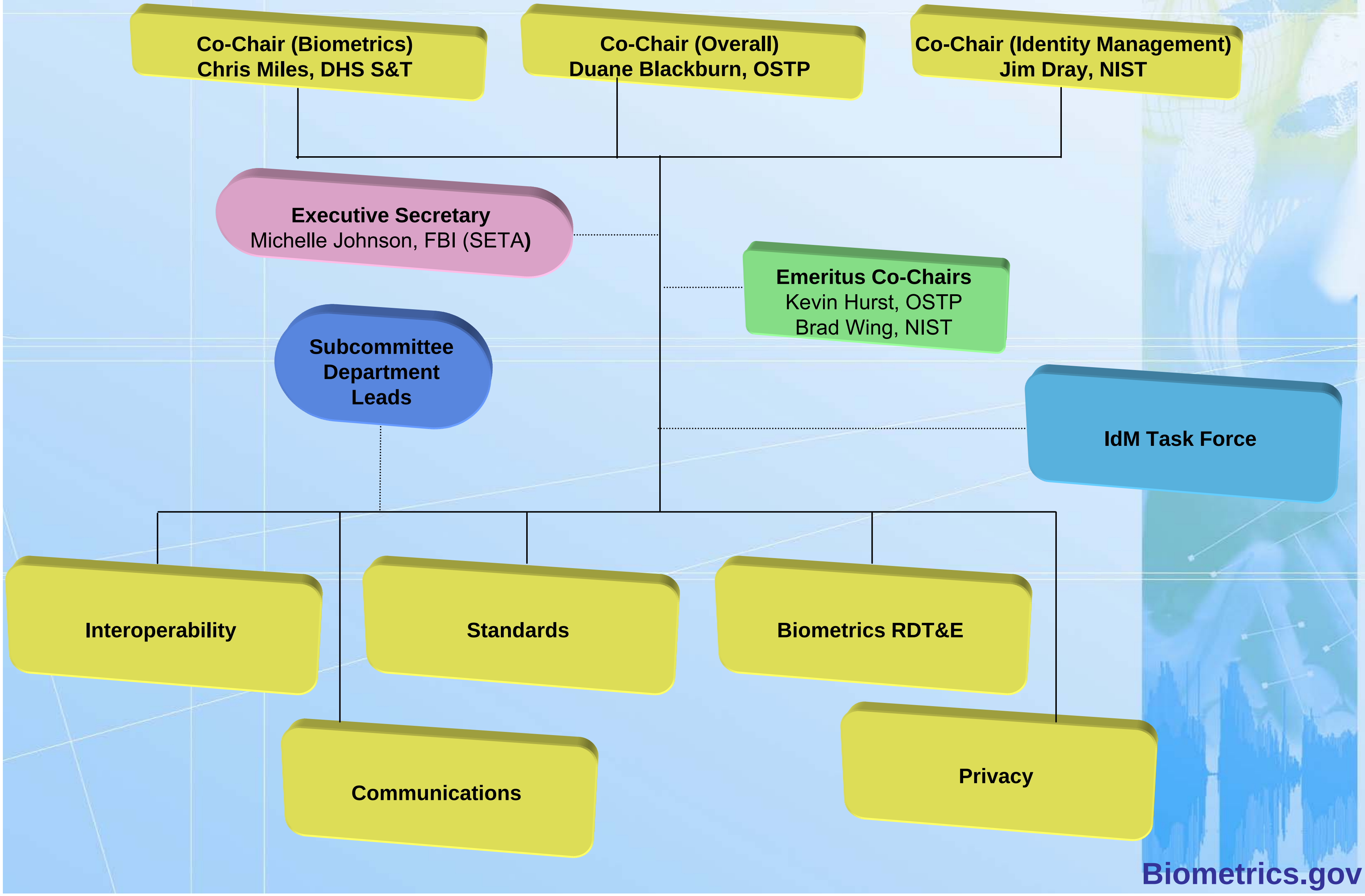
Goals:

- USG-wide biometric system of systems
- Community able to meet other government and private sector needs
- Expansion to IdM

Deliverables

- Interoperable Systems
- USG-wide plans for standards, RDT&E, privacy & communications
- Enhanced operational capabilities

NSTC Subcommittee on Biometrics & IdM



Co-Chair (Biometrics)
Chris Miles, DHS S&T

Co-Chair (Overall)
Duane Blackburn, OSTP

Co-Chair (Identity Management)
Jim Dray, NIST

Executive Secretary
Michelle Johnson, FBI (SETA**)**

Emeritus Co-Chairs
Kevin Hurst, OSTP
Brad Wing, NIST

Subcommittee Department Leads

IdM Task Force

Interoperability

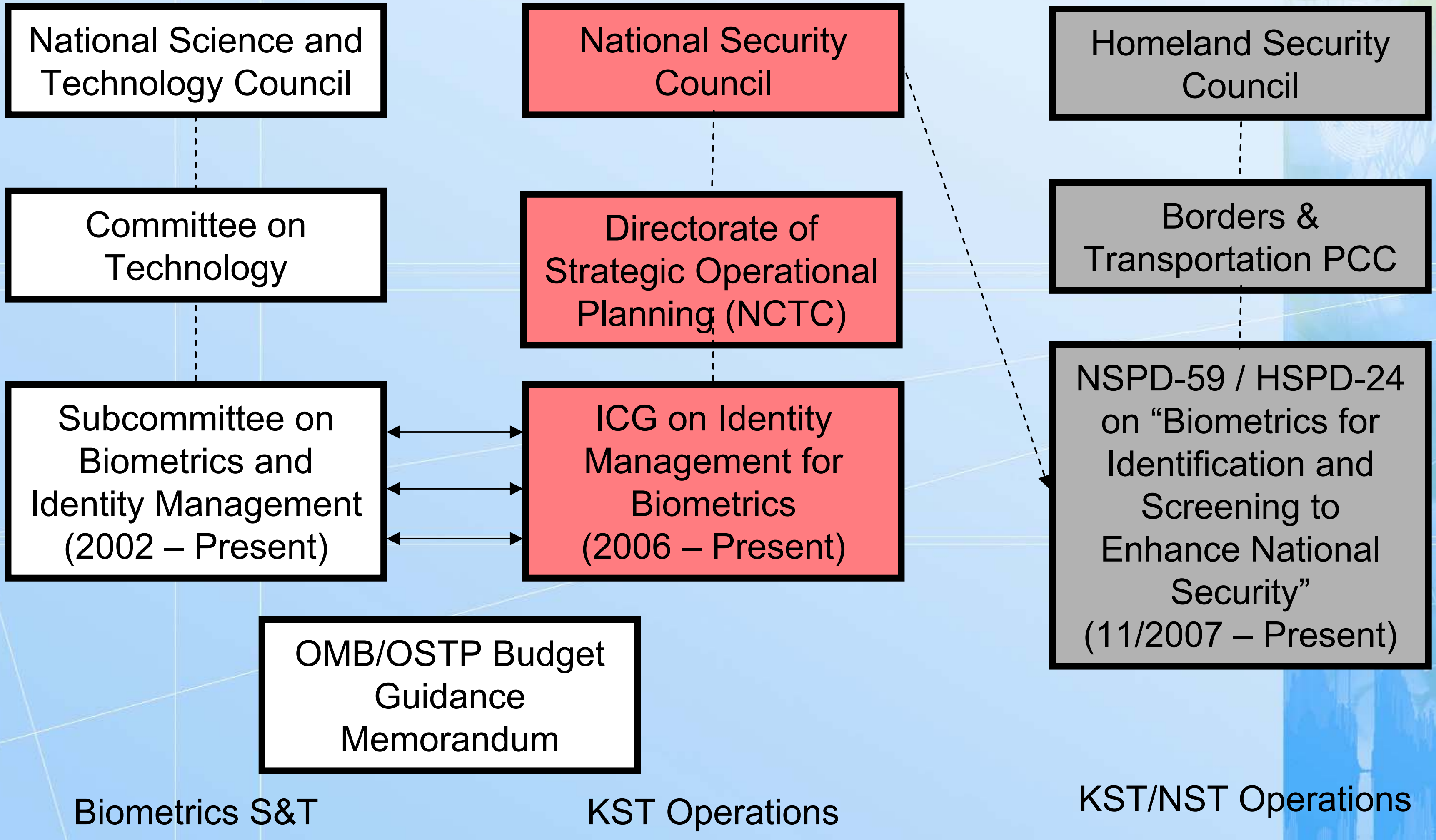
Standards

Biometrics RDT&E

Communications

Privacy

USG Biometrics Coordination - Organizational



National Science and Technology Council

Committee on Technology

Subcommittee on Biometrics and Identity Management (2002 – Present)

OMB/OSTP Budget Guidance Memorandum

Biometrics S&T

National Security Council

Directorate of Strategic Operational Planning (NCTC)

ICG on Identity Management for Biometrics (2006 – Present)

KST Operations

Homeland Security Council

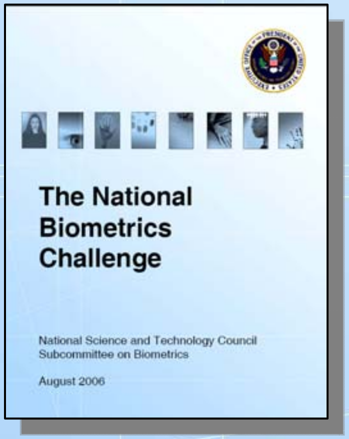
Borders & Transportation PCC

NSPD-59 / HSPD-24 on “Biometrics for Identification and Screening to Enhance National Security” (11/2007 – Present)

KST/NST Operations

Biometrics.gov

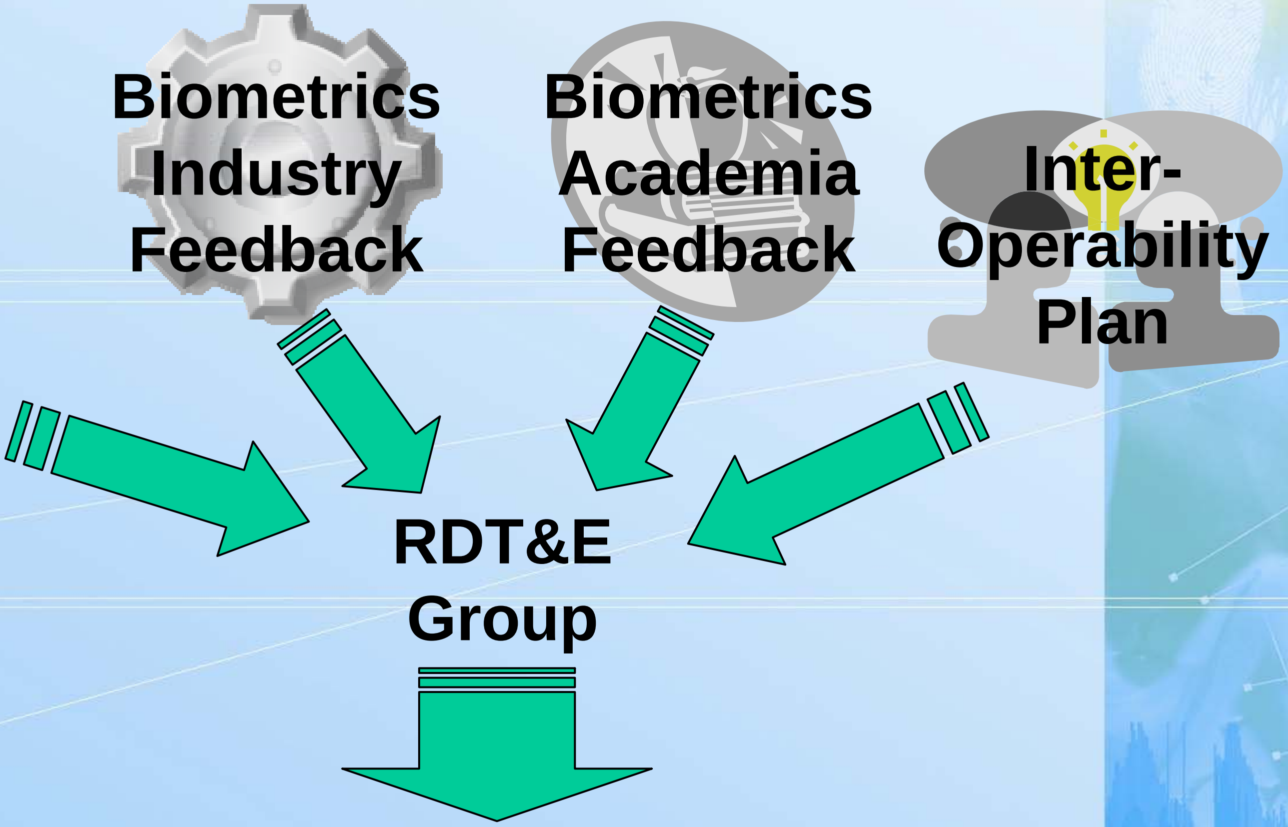
Advancing Technology



The National Biometrics Challenge

National Science and Technology Council
Subcommittee on Biometrics

August 2006



Biometrics Industry Feedback

Biometrics Academia Feedback

Inter-Operability Plan

RDT&E Group

Critical Priorities	Necessary Priorities	Recommended Priorities

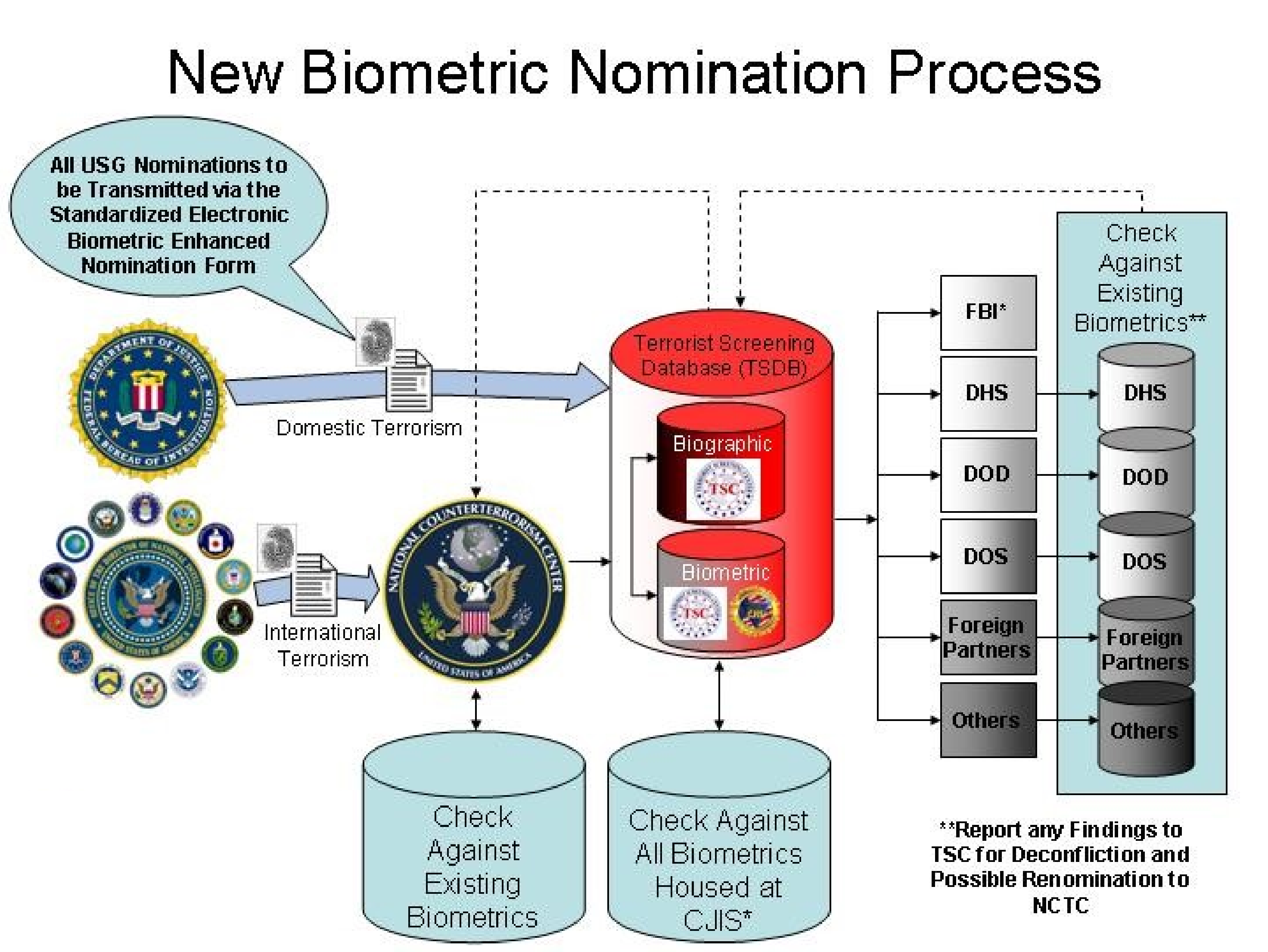
Registry of USG Recommended Biometric Standards

Sample Recommendation:

Table 1 - Registry of Biometric Data Collection, Storage, and Exchange Standards

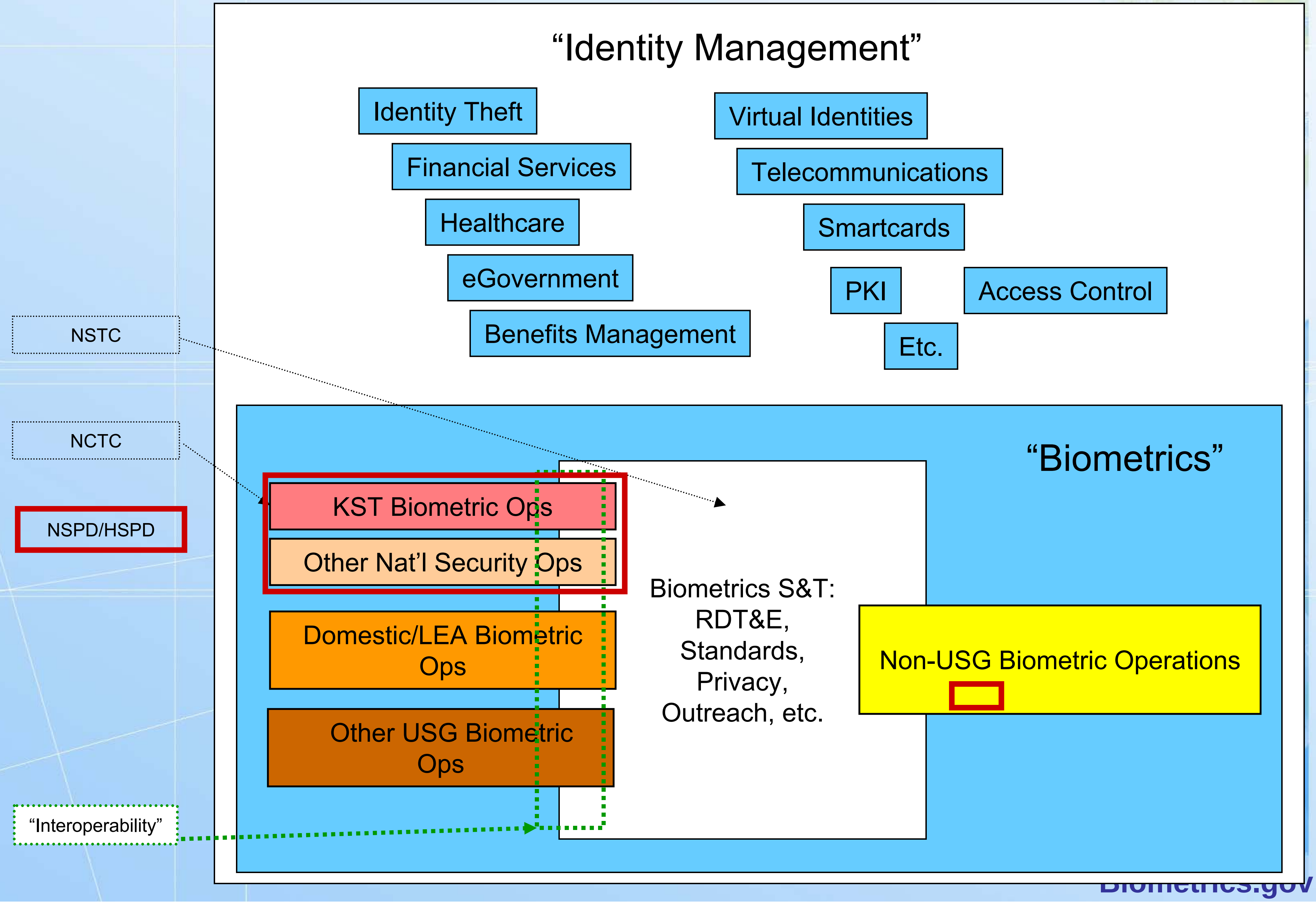
#	Validity period	Biometric data	Domain of applicability	Recommended standards	Notes
	Iris Recognition				
13.	October 2007 – current	Iris images	Capture, storage and exchange of data (e.g., enrollment or registration)	The rectilinear image format of ISO/IEC 19794-6:2005 or ANSI/NIST-ITL 1-2007, Type 17	If lossy compression is applied to iris images the compression ratio shall not exceed 6:1. For compression algorithms without a bit-rate parameter (e.g., JPEG), this may require iteration over the compression "quality" parameter. The INCITS 379:2004 standard shall not be used. The ANSI/NIST-ITL 1-2007, Type 17 format is a strict derivative of ISO/IEC 19794-6:2005, and may be used as an alternative. Other standards, including those enumerated below shall not be used as a substitute for the required standard; they may be used only in addition: All ISO/IEC 19794-6:2005 polar image formats. Irises stored in any of the polar image formats of ISO/IEC 19794-6:2005 may be retained only if their rectilinear image parents are also retained.

Interoperability Plan for KSTs*


New Biometric Nomination Process
All USG Nominations to be Transmitted via the Standardized Electronic Biometric Enhanced Nomination Form
Domestic Terrorism
International Terrorism
Terrorist Screening Database (TSDB)
Biographic
TSC
Biometric
TSC
Check Against Existing Biometrics
Check Against All Biometrics Housed at CJIS*
FBI*
DHS
DOD
DOS
Foreign Partners
Others
Check Against Existing Biometrics**
DHS
DOD
DOS
Foreign Partners
Others
**Report any Findings to TSC for Deconfliction and Possible Renomination to NCTC

* This is the plan for KSTs only. NSTs and other data sharing is managed differently

Biometrics and Identity Management



“Identity Management”

- Identity Theft
- Financial Services
- Healthcare
- eGovernment
- Benefits Management
- Virtual Identities
- Telecommunications
- Smartcards
- PKI
- Access Control
- Etc.

“Biometrics”

- KST Biometric Ops
- Other Nat’l Security Ops
- Domestic/LEA Biometric Ops
- Other USG Biometric Ops

Biometrics S&T: RDT&E, Standards, Privacy, Outreach, etc.

Non-USG Biometric Operations

NSTC

NCTC

NSPD/HSPD

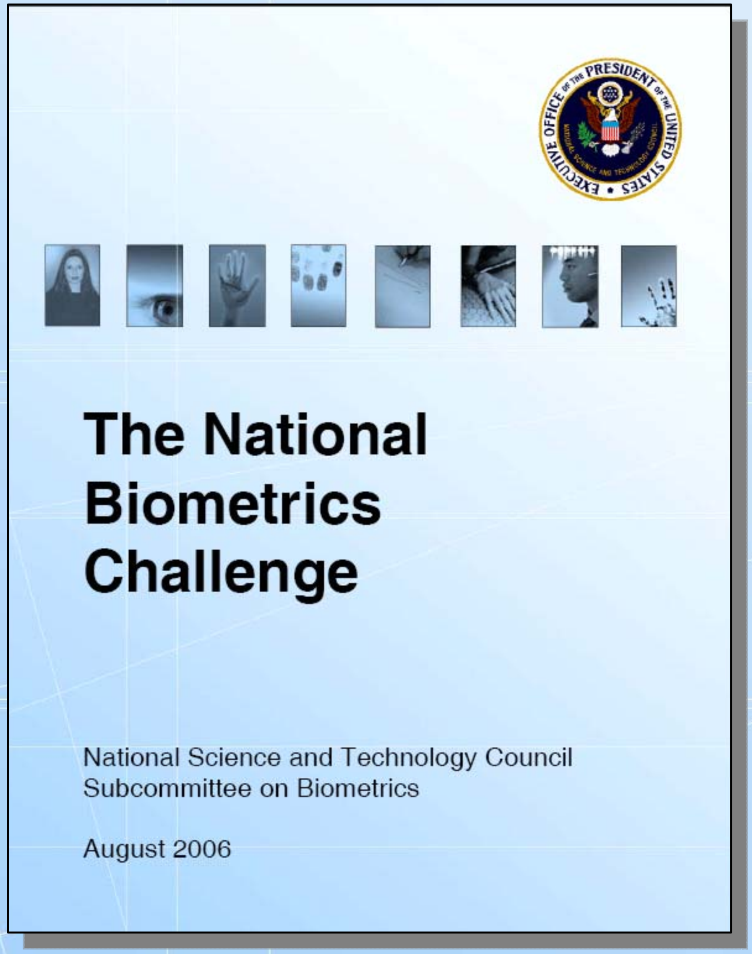
“Interoperability”

Research, Development, Test & Evaluation (RDT&E) Working Group

Chris Miles
DHS S&T

September 24, 2008

The National Biometrics Challenge



The National Biometrics Challenge

National Science and Technology Council
Subcommittee on Biometrics

August 2006

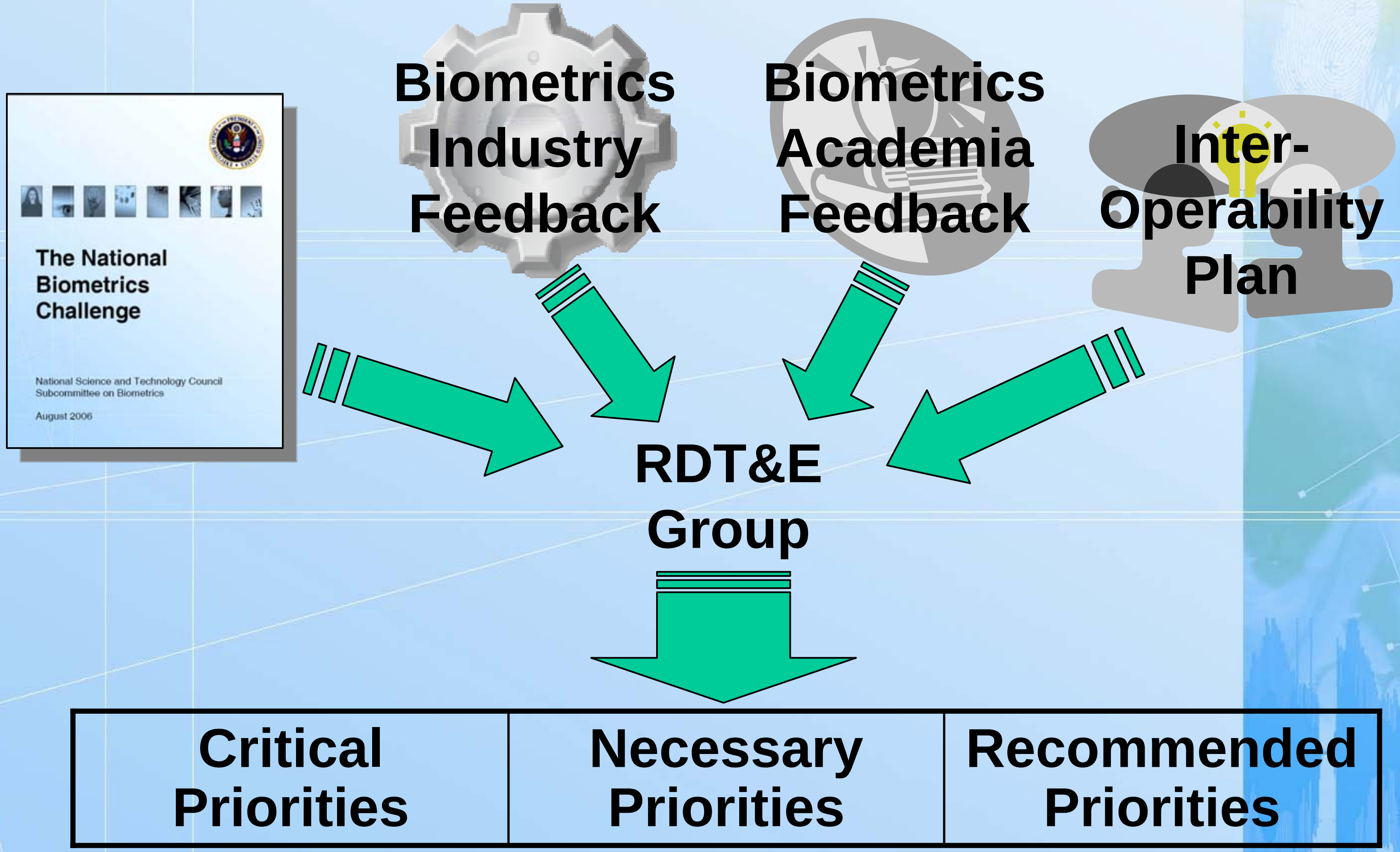
- Released in August 2006
- Continues to serve as a robust list of common challenges
- Provides an analysis of:
  - Unique attributes of biometrics
  - Market forces and societal issues
  - Advances required for next-generation capabilities
  - Communications and Privacy
  - Government’s Role in Biometrics

Outstanding Technology Needs

	Biometrics Challenges	National Security	Homeland Security & Law Enforce.	Enterprise & e-Gov Services	Personal Information & Business Trans.
5.1 Biometric Sensor Challenges	Mobile and Harsh Environments	x	x		
	Non-cooperative Persons at Distances	x	x		
	Relaxed Conditions	x	x		
	Revocable Templates	x	x	x	x
	Next Generation Sensors	x	x	x	x
5.2 Biometric System Challenges	Insensitivity to Operational Environments	x	x	x	x
	Modeling/Design/Selection Tools	x	x	x	x
	Intuitive Interfaces	x	x	x	x
	Multi-modal Enrollment and Recognition		x	x	x
	Return on Investment Models	x	x	x	x

Accomplishing the Technology Needs

A multi-year, multi-agency biometrics RDT&E research agenda was developed



The National Biometrics Challenge

National Science and Technology Council
Subcommittee on Biometrics

August 2006

Biometrics Industry Feedback

Biometrics Academia Feedback

Inter-Operability Plan

RDT&E Group

Critical Priorities

Necessary Priorities

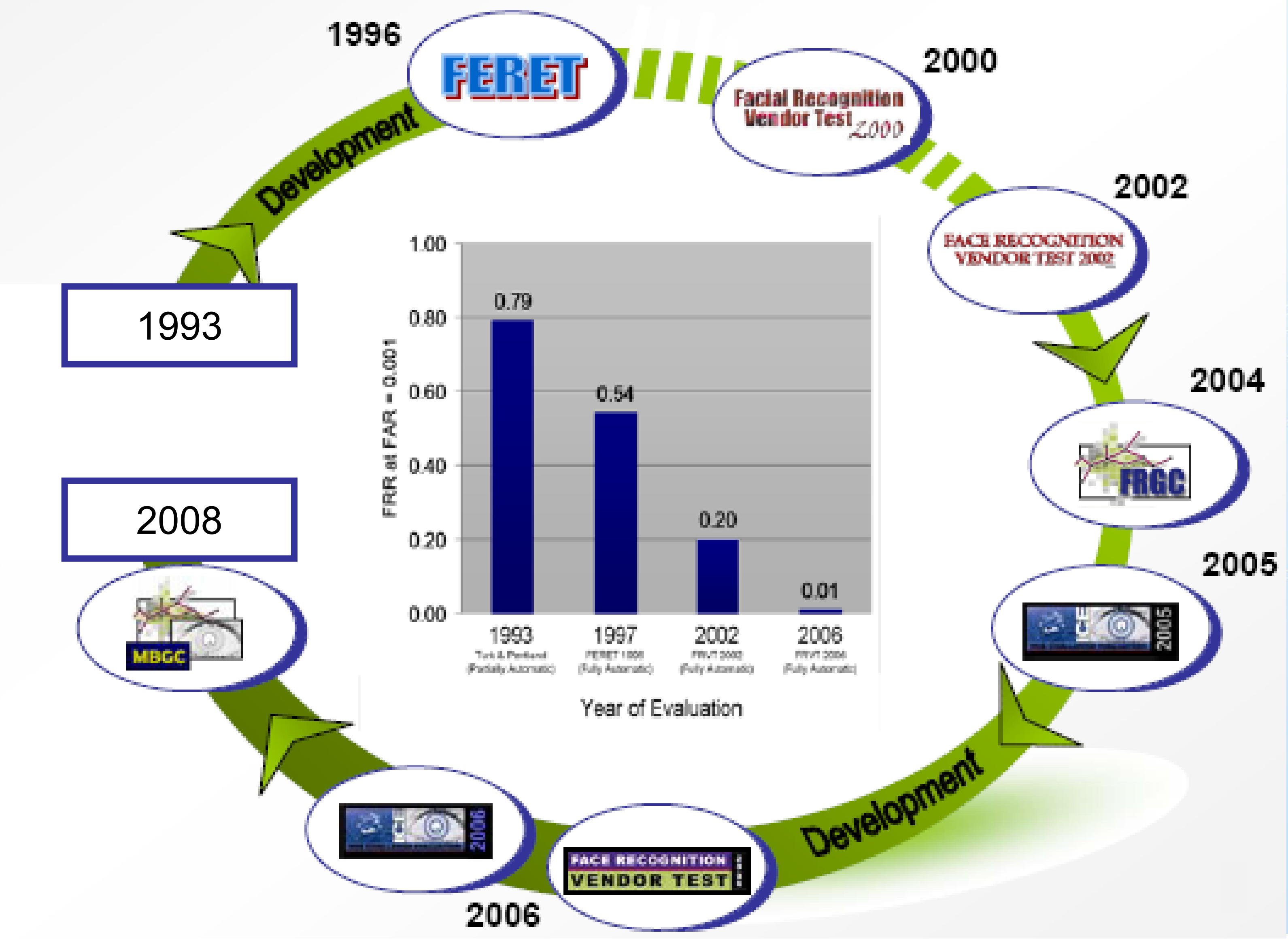
Recommended Priorities

Critical Priorities

RDT&E that Absolutely Must be Done to Accomplish Critical Needs:

- Fast and Intuitive Rolled-Equivalent Fingerprints
- Improved Traditional Sensors
- Traditional Sensors in Mobile and Harsh Environments
- Stand-off Face and Iris Sensors and Matching Algorithms
- Multi-Modal Biometrics in Ideal and Non-Ideal Conditions
- Middleware Techniques/Standards for “Plug-and-Play” Sensors
- Test & Evaluation of Traditional Sensors and Algorithms
- Analysis of System Scalability Issues and Research

T&E: Multiple Biometrics Grand Challenge (MBGC) & Evaluation (MBE)



More Info.
NIST Session
09/25
9:00 AM

Biometrics.gov

T&E: International Usability Workshop

The International Workshop on Usability and Biometrics
June 23-24, 2008

U.S. Department of Homeland Security

US-VISIT
Keeping America's Doors Open and Our Nation Secure

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Evaluation of a set of usability guidelines to:

- enhance performance
- improve user satisfaction/acceptance
- provide consistency

Six usability research studies:

- user habituation or acclimatization
- counter height and anthropometrics
- instructional materials
- adaptable devices for accessibility
- international symbols
- relationship of counter height and angle of fingerprint scanners
- face overlays

More Info.
NIST Session
09/25
10:40 AM

http://zing.ncsl.nist.gov/biousa/html/workshop08.html

Necessary Priorities

RDT&E that Must be Done to Accomplish Needs:

- Revocable/Replaceable Biometrics
- Enhanced Non-Traditional Sensors and Algorithms
- Automated Environment-Adjusting Sensors
- Enhancing Sub-Optimal Data (Improving Data Quality)
- Lights-Out, Real Time, Latent Screening
- Collection/Analysis/Feedback of Large Perimeter Security/Chokepoints

Recommended Priorities

RDT&E that Adds Additional Technology Features:

- Enhanced Traditional Algorithms
- Enhanced Non-Traditional Algorithms
- Contactless and/or Self-Sterilizing Contact Fingerprint Sensors
- Application-Based Scenario and Performance Testing
- Human Factors Analysis and Future Adoption Guidelines
- Common Applications Return on Investment (ROI) Models
- Portable matching-verification-credentialing (match on card, non-fixed locations, etc.)

Standards & Conformity Assessment Working Group (SCA WG)

Michael D. Hogan
National Institute of Standards and Technology

September 24, 2008

Our Goals

- A USG-wide ability to collect, store, and exchange biometrics based upon adopted standards and testing in support of immediate and future agency missions.
- A robust testing infrastructure available to support biometric standardization, grant guidance and procurement.

Your Success Depends on Knowing

- ►What biometric standards have been adopted for USG-wide use?
- ► What biometric standards will be adopted for USG-wide use?
- ►What kinds of USG biometric testing are required?
- ►What kinds of USG biometric testing will be required?

Standards and Conformity Assessment

- ►***Standards***, often, specify requirements.
- ►***Conformity Assessment (CA)*** determines whether a product, service or system has fulfilled all of those requirements.

Standards and Conformity Assessment Working Group (SCA WG)

- ►NSTC Subcommittee on Biometrics and Identity Management has worked on biometric standards and related testing issues from its inception in 2002.
- ►The Subcommittee established the SCA WG in late 2005.

Standards and Conformity Assessment Working Group (SCA WG)

- ►Respond to the biometrics standards and related testing issues identified in *The National Biometrics Challenge.*
- ►Develop interagency consensus on biometric standards-related items required to enable the interoperability of various Federal biometric applications.

Subcommittee Timeline

►August 2006 – *The National Biometrics Challenge*

http://www.biometrics.gov/NSTC/Publications.aspx

►September 2007 – *NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards*

http://www.biometrics.gov/Standards/Default.aspx

►June 2008 – *Registry of USG Recommended Biometric Standards*

http://www.biometrics.gov/Standards/Default.aspx

NSTC Policy Subcommittee Actions

- Review and recommend standards for use across the USG.
- Develop and maintain a registry of USG recommended biometric standards.
- Work to advance adoption of recommended standards by agencies.

NSTC Policy
Agency Actions

- ►Support voluntary biometric standards development activities.
- ►Develop harmonized biometric testing programs in support of procurements.
- ►Build and operate biometric systems using recommended standards.

Types of Standards in the Registry

- biometric data collection, storage, and exchange standards
- biometric transmission profiles
- biometric identity credentialing profiles
- biometric technical interface standards
- biometric conformance testing methodology standards
- biometric performance testing methodology standards

Registry of USG Recommended Biometric Standards

- ►As new standards, and revisions to existing standards, are approved by the standards developers, they will be evaluated by the Subcommittee for USG-wide use and may be added to the Registry.
- ►Two biometric modalities are clear priorities for addition to the Registry:
  - ►Voice
  - ►DNA

Action Plan

- ►The SCA WG is developing an *Action Plan* that tracks USG actions in support of the development of biometric standards and testing.
- ►For Conformity Assessment, the *Action Plan* includes:
  - ►development of test tools for the recommended standards;
  - ►2nd party testing;
  - ►accreditation of 3rd party testing laboratories;
  - ►certification of test results.

Conformity Assessment - Testing

- ►***Conformance testing*** - process of checking, via test assertions, whether an implementation faithfully implements the standard or profile.
- ►***Performance testing*** - measures the performance characteristics of an implementation such as system error rates, throughput, or responsiveness, under various conditions.

Conformance Test Tools for Biometric Standards

- ►2005 – DoD and NIST release two cross tested test tools for BioAPI (INCITS 358-2002).
  - ► http://www.itl.nist.gov/div893/biometrics/BioAPI_CTS/index.htm
  - ► http://www.biometrics.dod.mil/CurrentInitiatives/Standards/TestingToolsets.aspx
- ►2006 – NIST establishes a Minutiae Exchange Interoperability Test for INCITS 378-2004.
  - ► http://fingerprint.nist.gov/minex/
- ►August 2008 - NIST releases a conformance testing architecture and test tool for CBEFF Patron Format A (specified in INCITS 398-2008).
  - ► http://www.itl.nist.gov/div893/biometrics/CBEFF_PFA_CTS/index.htm
  - ► See NIST demonstration of the released architecture and test tool, as well as a pre-release version of an advanced testing architecture for biometric data interchange standards, at booth #210.

Who Performs Conformity Assessment (CA)?

- ►*first party* – seller or manufacturer;
- ►*second party* – purchaser or user;
- ►*third party* – an independent entity that has no interest in transactions between the 1st and 2nd parties.

USG Approach to CA for Biometric Standards

- ►2nd party or 3rd party testing should be used when the risks associated with non-conformity are moderate to high.
- ►To achieve a high level of assurance of standards conformance by biometric systems and components:
  - ►2nd party testing is being used by various USG biometric applications; and
  - ►3rd party testing is being planned for use by some USG biometric applications.

Qualified Product Lists (QPLs) of Biometric Products

- ►Approved Product List of Fingerprint Scanners and Card Readers for the FBI's IAFIS

  http://www.fbi.gov/hq/cjisd/iafis/cert.htm

- ►Approved Product List for FIPS 201(PIV)

  http://www.idmanagement.gov/

- ►TSA QPL for Testing of Biometrics Access Control Systems

  http://www.biometricgroup.com/QPL/

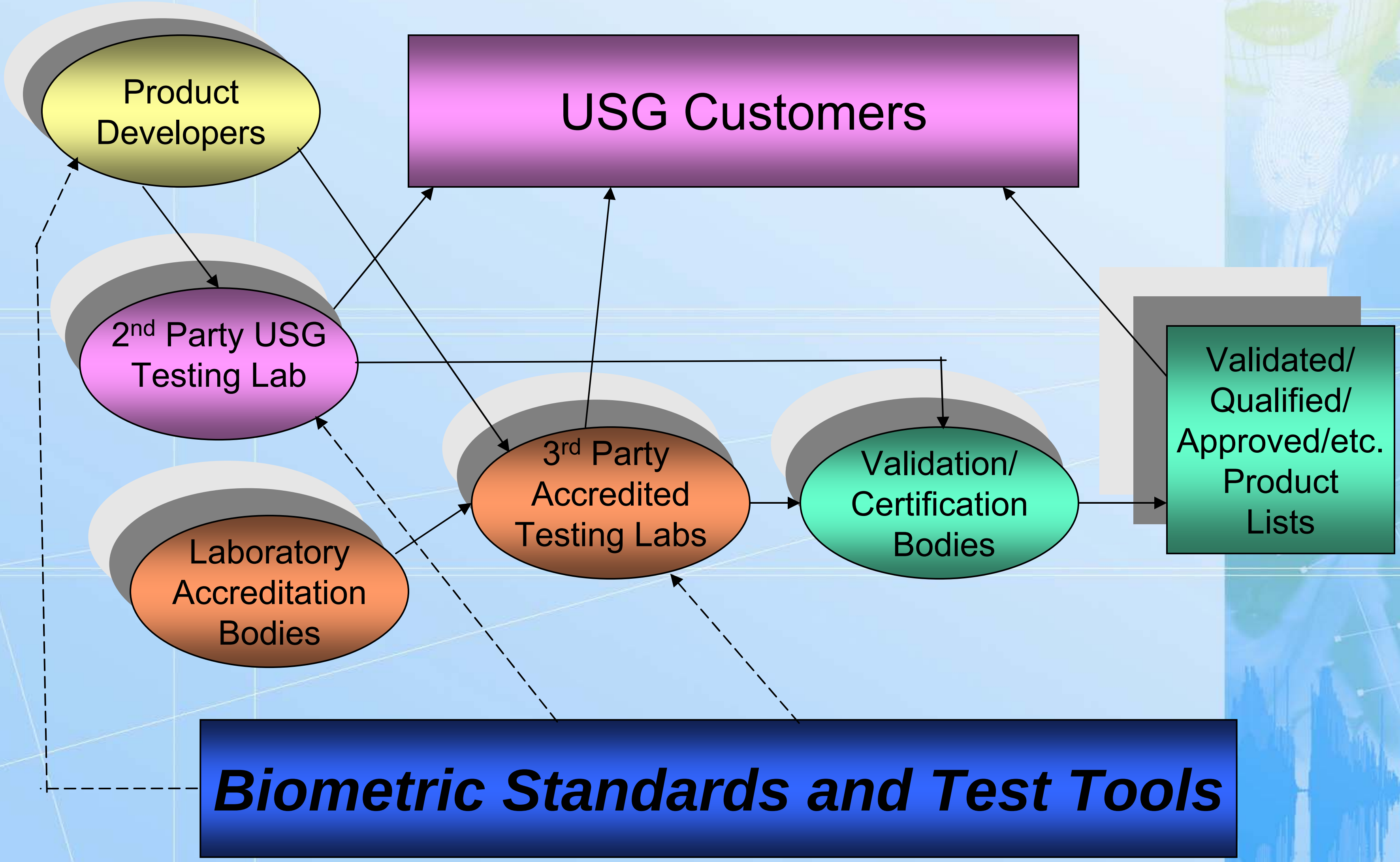
Planning for USG 3rd Party Testing

- July 1, 2008 – NIST Public Workshop on Laboratory Accreditation for Biometrics Testing
- Intended audience – stakeholders (e.g., test laboratory, equipment supplier, government agency, researcher) interested in biometric technologies to verify the identity of individuals to gain access to information or secure areas
- Contact: Brad Moore brad.moore@nist.gov

Present Situation

- ►Groundbreaking USG-wide standards selection process is now in place.
- ►Augmenting the existing USG CA capabilities in support of the recommended standards is now underway.

Robust Standards & CA Infrastructure



Product Developers

USG Customers

2nd Party USG Testing Lab

3rd Party Accredited Testing Labs

Validation/ Certification Bodies

Validated/ Qualified/ Approved/etc. Product Lists

Laboratory Accreditation Bodies

Biometric Standards and Test Tools

Questions?

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Bridging the Gap

Linking Biometric Government Systems

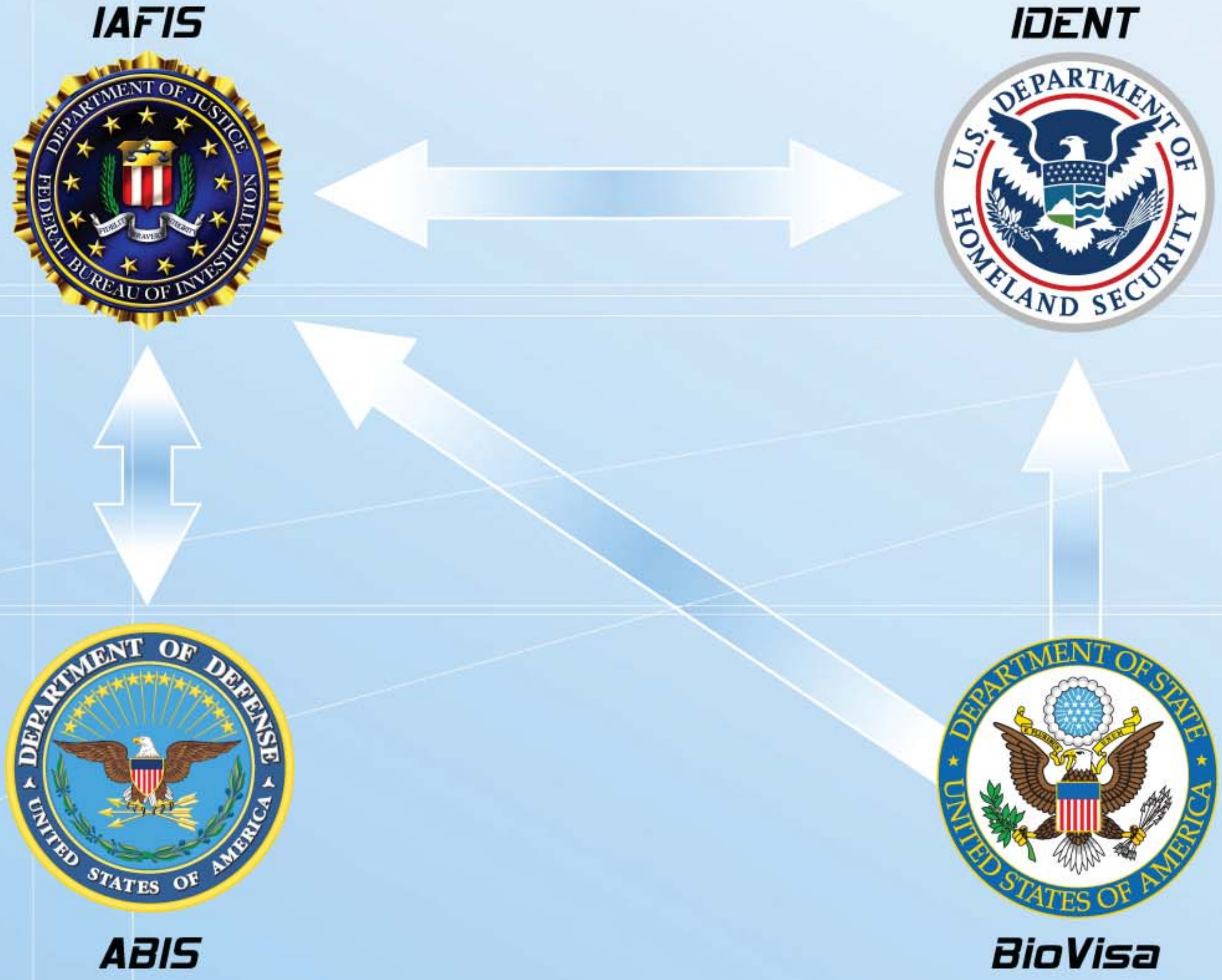
Kimberly J. Del Greco
FBI Criminal Justice Information Services Division

September 24, 2008

Report on Interoperability – How do we Bridge the Gap

- Provides overview of the 2007 and 2008 efforts to bridge the gap on sharing Known or Suspected Terrorist (KST) record information.
- Large Screening Agencies:
  - FBI
  - DOD
  - DHS
  - DOS
- Provides top-level description of the new KST architecture that federal agencies will be adapting their systems to support.

Where Are We Today?



IAFIS

IDENT

ABIS

BioVisa

Way Forward

- ► 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 KST watch list

Partnering to Bridge the Gap

Patterns of Success

NSTC Interoperability Subgroup
Focus - KST

- ► January 2007 worked with/through NCTC
- ► Established several options and factors
- ► November 2007 the Interagency Coordination Group (ICG) approved the KST Interoperability Business Process

Interoperability Business Process

- ► Improve coordination, integration, and synchronization of biometric based records
- ► Standardized Electronic, biometrically-enabled nomination form;
- ► Successful implementation of comprehensive terrorist identity records

Interoperability Business Process

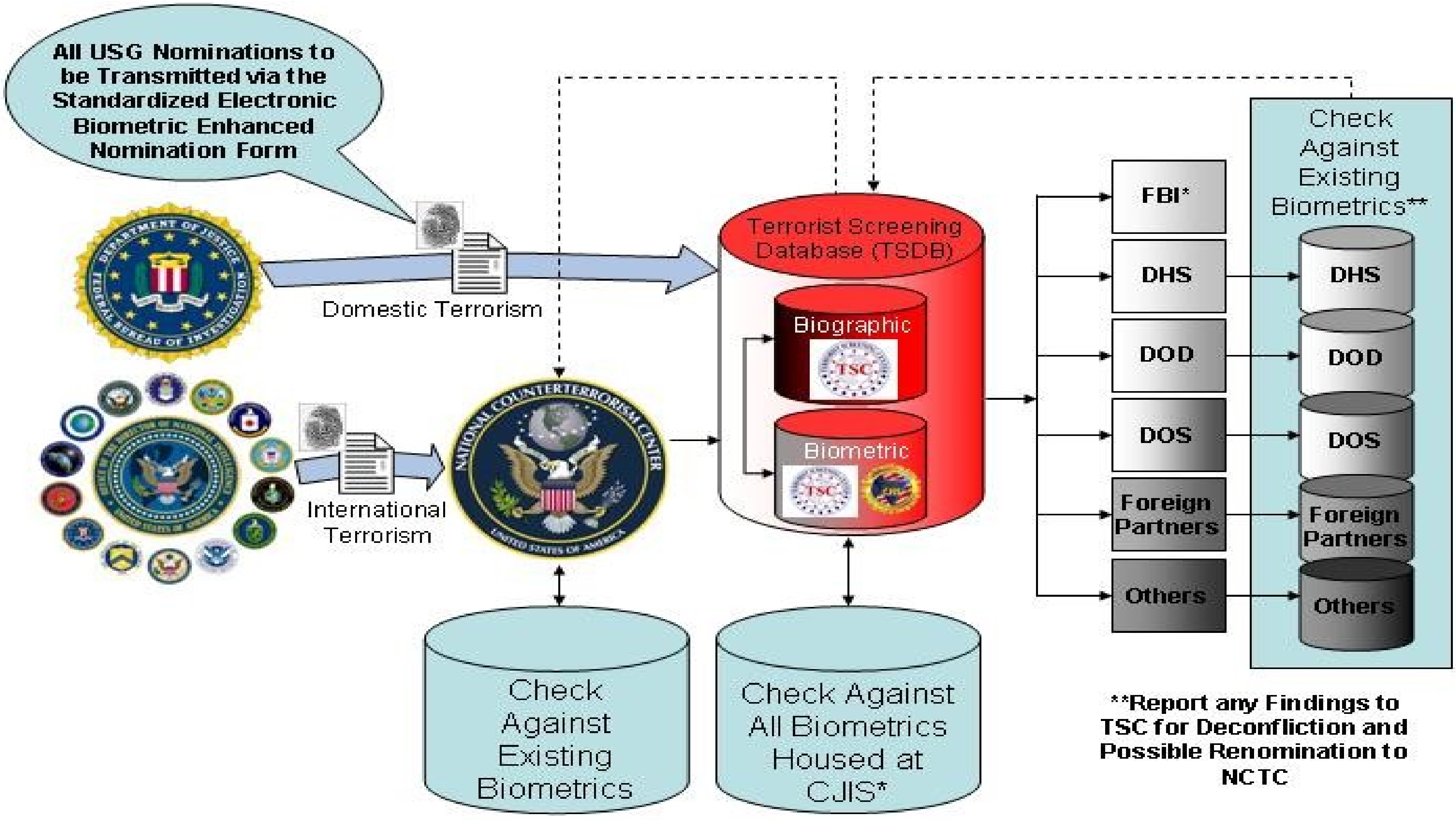
► Institution of an unique numbering system

► Establish interagency auditing capability; and

► Improve processes to resolve conflicts in identity information

Interoperability Plan for KSTs

New Biometric Nomination Process

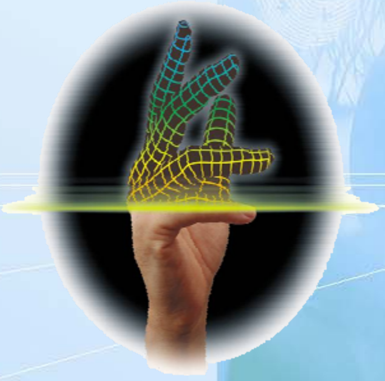

All USG Nominations to be Transmitted via the Standardized Electronic Biometric Enhanced Nomination Form
Domestic Terrorism
International Terrorism
Terrorist Screening Database (TSDB)
Biographic
Biometric
FBI*
DHS
DOD
DOS
Foreign Partners
Others
Check Against Existing Biometrics**
DHS
DOD
DOS
Foreign Partners
Others
Check Against Existing Biometrics
Check Against All Biometrics Housed at CJIS*

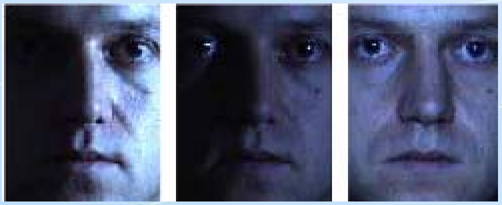
**Report any Findings to TSC for Deconfliction and Possible Renomination to NCTC

Interoperability

- All Departments move towards collection of primary Biometrics

  - Finger





  - Face

  - Iris

Biometrics.gov

Breakdown

1. Standardized electronic nominations - biographic and biometric are made by nominating organizations to NCTC

2. NCTC will implement a phased approach to receiving, matching, and storing of biometric nominations

Breakdown

3. New nominations will be forwarded to TSC for inclusion into their repository.

4. TSC will ensure both biographic and biometric identifiers are made available NEAR REAL TIME for identification and screening to DOD, DOJ, DHS, DOS.

Interoperability

February 2008 Counterterrorism Screening Group approved the Interoperability Business Process

Interoperability for National Security

- ► June 5, 2008 - National Security Presidential Directive/NSPD - 59

  Homeland Security Presidential Directive/HSPD – 24

Common strategy to achieve a robust biometric capability to identify those individuals who pose a national security threat to the United States.

Interoperability for National Security

- Two areas
  - KSTs - Known or Suspected Terrorists
  - NSTs – Individuals who may pose a threat to National Security
- Attorney General Authority

Interoperability for National Security

►Roles and Responsibilities

►COLLECTION

►ANALYSIS

►USE

►STORAGE

►EXCHANGE

Biometrics.gov

Roles and Responsibilities

- **Use common technology standards, protocols and interfaces**
- **Ensure compliance with laws, policies, and procedures**
- **Ensure KST biometric Information is provided to NCTC and TSC**

Looking into the Future

Closing the Gap

HSPD – 24
Implementation

- **The Attorney General, in coordination shall establish an action plan**
  - **setting forth a phased approach to address identified technology gaps**

Take Away

►9/11 iniated

►KSTs top priority

►KST interoperability approach

►NSTs

►Closing gaps – Government networking

►Private Sector

National Science and Technology Council Task Force on Identity Management

James Dray
National Institute of Standards and Technology

September 24, 2008

Task Force Compositiion

- Six month effort (January 1 – July 2)
- Co-chairs
  - Duane Blackburn (OSTP)
  - Judy Spencer (GSA)
  - Jim Dray (NIST)
- Working groups
  - Drafting team
  - Data Collection and Analysis
  - Digital Identity
  - Grid
  - Privacy and Legal
- Participating agencies included DHS, DOD, DOS, DOJ, HHS, SSA, FTC, DOC, GSA, EOP, NSF, ODNI, NASA, FAA, VA

Task Force Process

- ► Weekly meetings every Thursday
- ► Special presentations
- ► Charter
  - ► Assess current IdM landscape
  - ► Develop vision for the “to be”
  - ► Develop recommendations to move forward

Challenges

- Much work had to be done in parallel
- Impossible to thoroughly capture the complex IdM landscape in six months
- Satisfying all equities: Law enforcement, intelligence, access control
- Privacy
- Agency desire for autonomy
- USG cannot dictate private sector IdM strategies but must interact with them

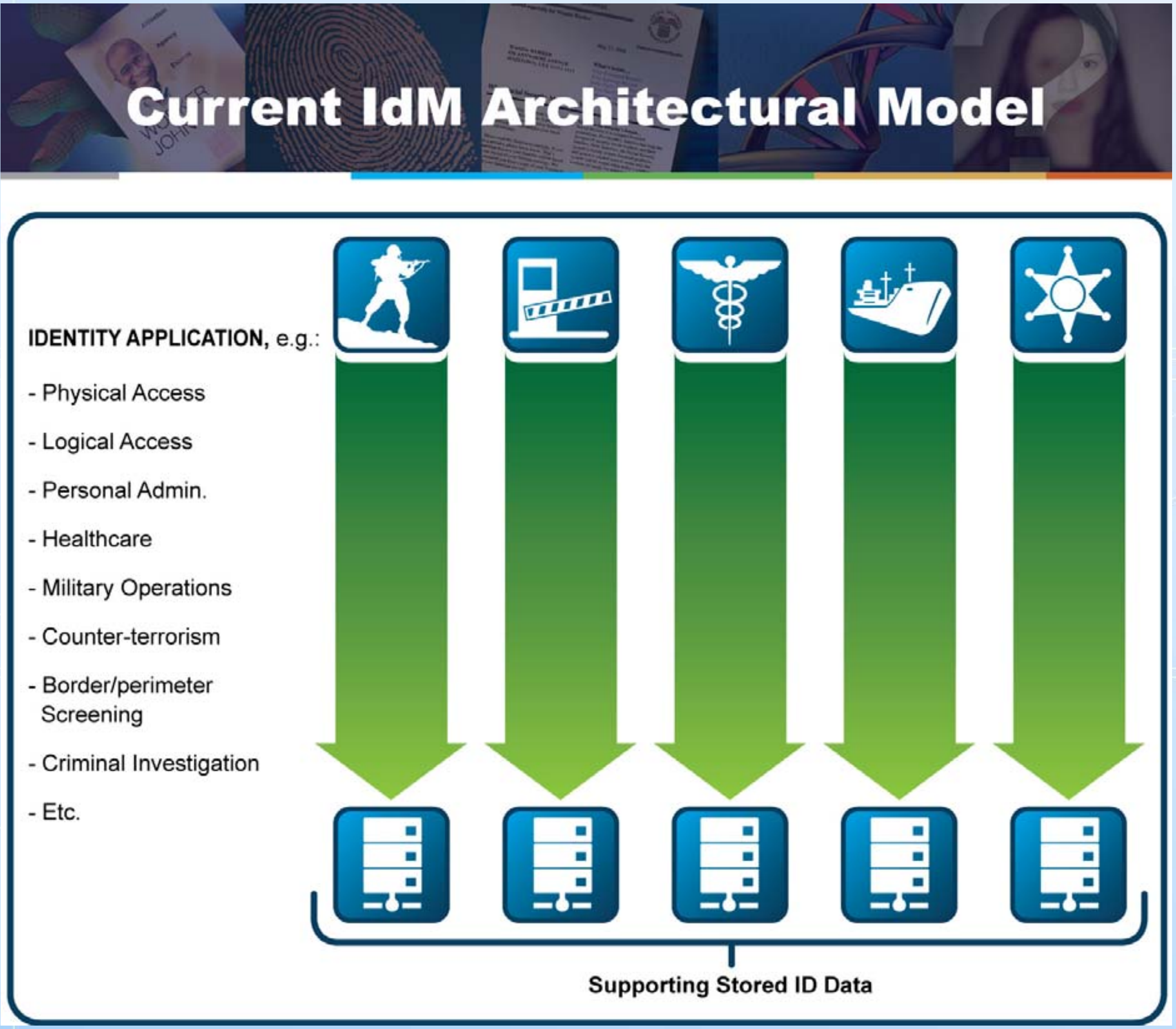
CIO Council Data Call

- First-order understanding of the IdM landscape
- Final Report Appendix G
- 18 responses covering 191 agencies/bureaus, 3400 individual systems
- The most common forms of information being collected for IdM are login alias, PIN/password, legal name, date of birth and social security number
- Few systems (~15%) or programs collect or use biometric-related data (e.g., fingerprints, iris or facial imaging) or use security questions or tokens

Summary Findings and Opinions

- No normative definition of “Identity Management”
- Governance process required
- Privacy can be enhanced by IdM
- Consolidated IdM vision will enable consistent application of appropriate privacy controls across the IdM landscape
- There will be no “one size fits all” solution – heterogeneous IdM systems will continue to evolve
- However, benefits can be achieved from a metaframework approach that promotes common technical standards and strategies

Current Landscape



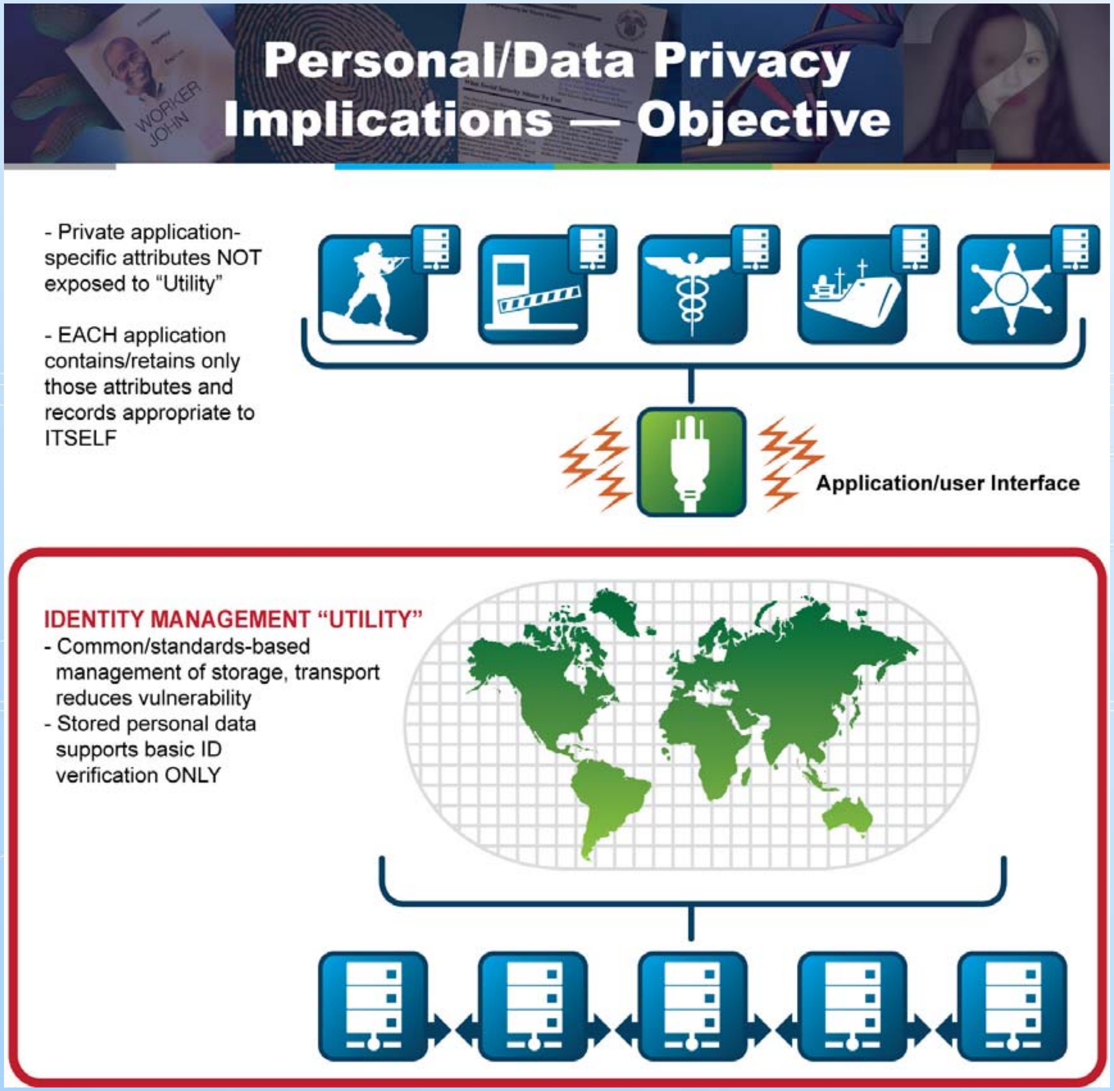
Current IdM Architectural Model

IDENTITY APPLICATION, e.g.:

- Physical Access
- Logical Access
- Personal Admin.
- Healthcare
- Military Operations
- Counter-terrorism
- Border/perimeter Screening
- Criminal Investigation
- Etc.

Supporting Stored ID Data

Privacy Implications



Personal/Data Privacy Implications — Objective

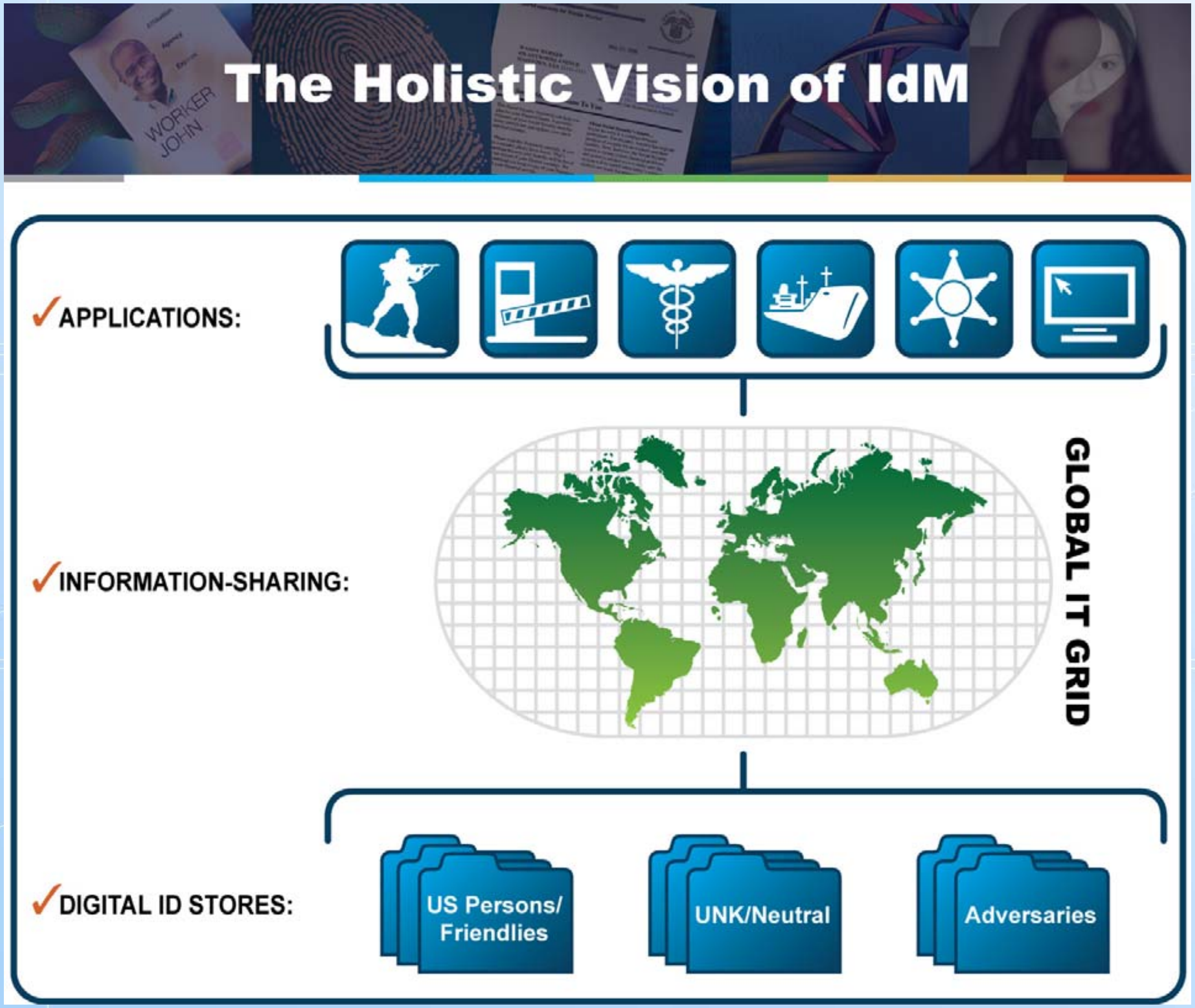
- Private application-specific attributes NOT exposed to “Utility”

- EACH application contains/retains only those attributes and records appropriate to ITSELF

IDENTITY MANAGEMENT “UTILITY”

- Common/standards-based management of storage, transport reduces vulnerability
- Stored personal data supports basic ID verification ONLY

Vision of the "To Be"



The Holistic Vision of IdM

✓APPLICATIONS:

✓INFORMATION-SHARING:

GLOBAL IT GRID

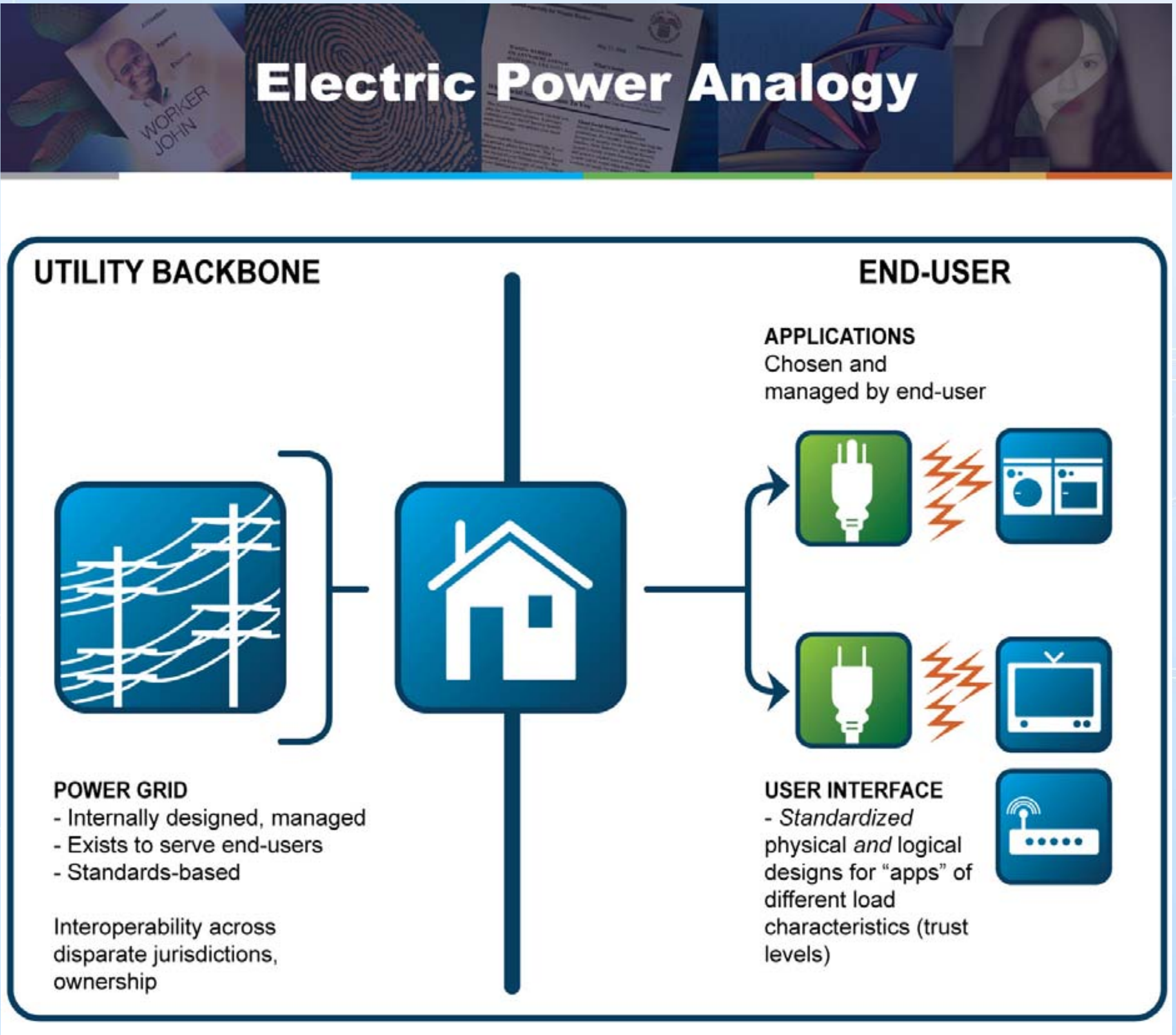
✓DIGITAL ID STORES:

US Persons/ Friendlies

UNK/Neutral

Adversaries

Identity Management Utility



Electric Power Analogy

UTILITY BACKBONE

END-USER

APPLICATIONS
Chosen and managed by end-user

POWER GRID
- Internally designed, managed
- Exists to serve end-users
- Standards-based

Interoperability across disparate jurisdictions, ownership

USER INTERFACE
- *Standardized* physical *and* logical designs for "apps" of different load characteristics (trust levels)

Don’t forget the Identity Management side session later today from 2:00 pm to 5:00 pm in Room 31/32!

Questions?

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Contacts

Overall	Duane Blackburn	OSTP	dblackburn@ostp.eop.gov	202-456-6068
RDT&E	Chris Miles	DHS S&T	Christopher.Miles@dhs.gov	(202) 254-6642
Standards	Mike Hogan	NIST	m.hogan@nist.gov	301-975-2926
Interoperability	Kim Del Greco	FBI	kimberly.delgreco@ic.fbi.gov	304-625-2400
Privacy	Peter Sand Niels Quist	DHS Privacy Office DOJ Office of Privacy & Civil Liberties	Peter.Sand@dhs.gov Niels.Quist@usdoj.gov	571-227-3813 202-616-5491
Communications	Kim Weissman	US-VISIT	Kimberly.weissman@dhs.gov	(202) 298-5026
IdM TF	Jim Dray	NIST	James.dray@nist.gov	(301) 975-3356