The National Biometrics Challenge 2011

James Loudermilk

Federal Bureau of Investigation

Larry Hornak

National Science Foundation

Update Co-Chairs

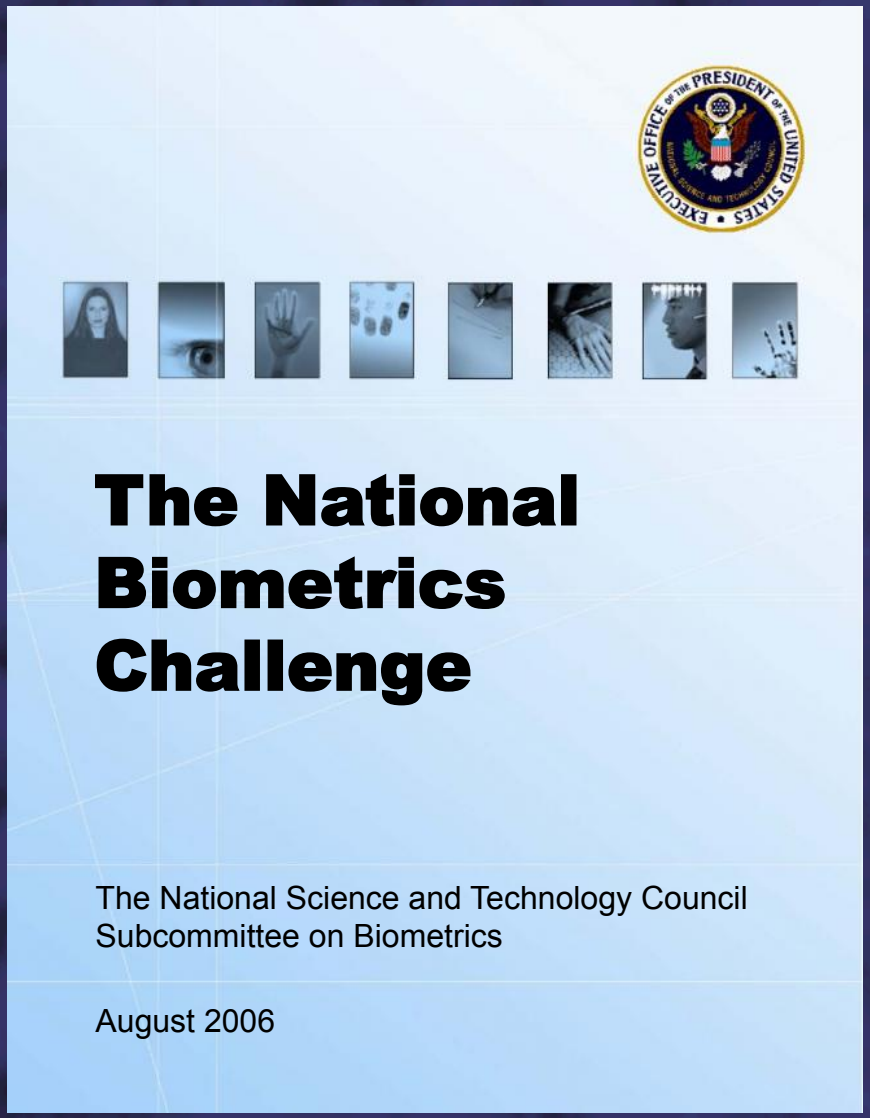
National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on Nov. 23, 1993. This Cabinet-level Council is the principal means by which the executive branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise.

- Chaired by the President,
- the Vice President,
- the Director of the Office of Science and Technology Policy,
- Cabinet Secretaries,
- Agency heads with significant science and technology responsibilities,
- and other White House officials

One of NSTC's primary objectives is to establish clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch.

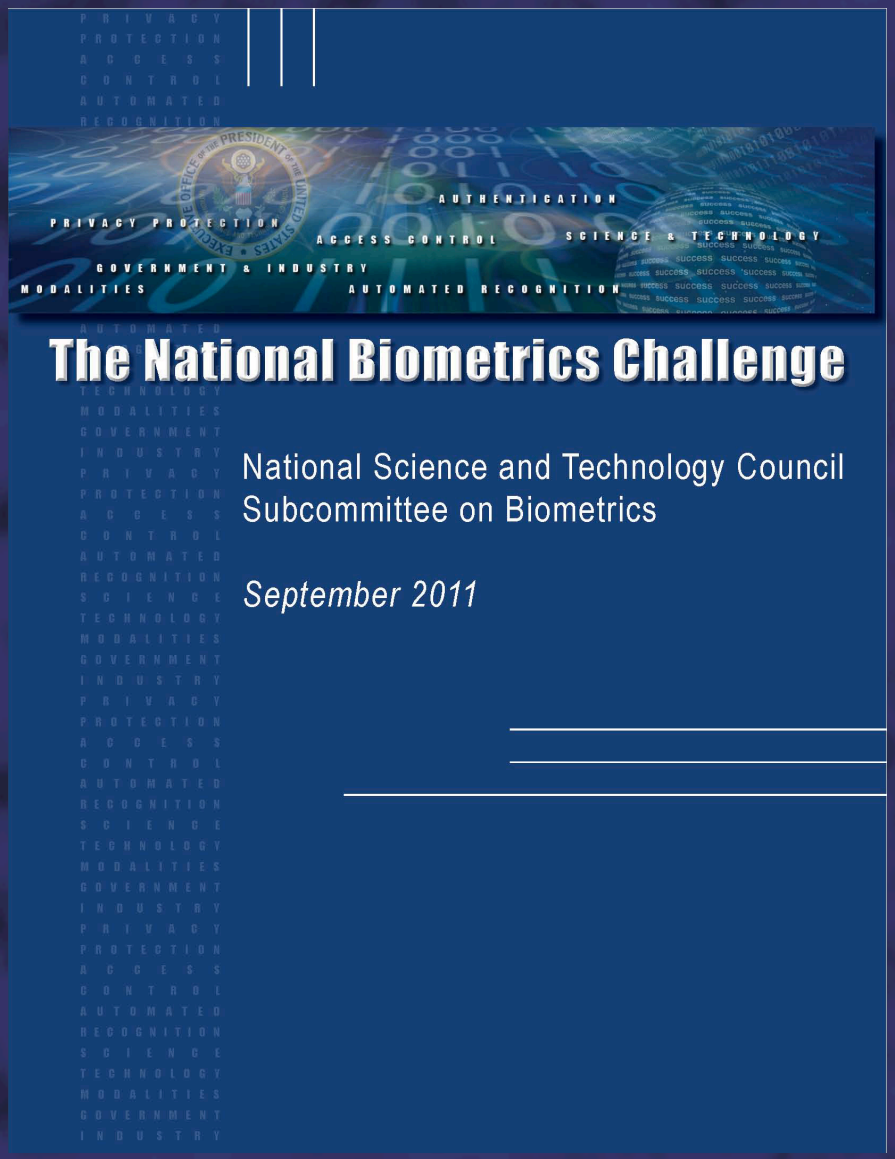
NSTC prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals.



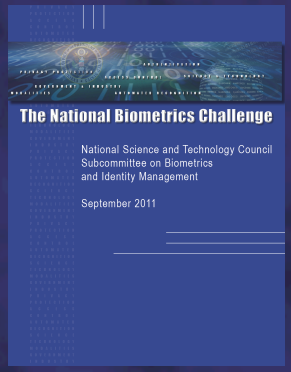
"The NSTC Subcommittee on Biometrics prepared and published the original *National Biometrics Challenge* in August 2006. That report identified key challenges in advancing biometrics development. It was based upon analysis of the unique attributes of biometrics, the market forces and societal issues driving implementation of biometrics and the advances required for next-generation capabilities. A further prioritization was done within the Subcommittee, and the top third of priorities received about 83 percent of federal funding."

Privacy and Privacy Protection - 2006

- "Facilitate the inclusion of privacy-protecting principles in biometrics system design" part of purpose of Subcommittee
- "development of consensus on social, legal, privacy and policy considerations"
- "Enable informed debate on why, how and when biometrics should and can be used"
- "enable their implementation to be consistent with privacy laws and widely accepted privacy principles"
- "Individuals have varied understandings, and place varied importance, on privacy and privacy protection. The biometrics community must further engage lawmakers, the legal community, and the public . . . Formulation and subsequent widespread acceptance of privacy-protection policies for biometric systems . . ."
- "Privacy-protective solutions that meet operational needs enhance public confidence in biometrics technology and safeguard personal information"
- "Communicate, in the appropriate form, the results of privacy assessments to demonstrate the practice and value of transparency"



"During the last five years, evolving mission needs, coupled with advances in technology, have necessitated a new look at research, development, test and evaluation (RDT&E) priorities. This 2011 update to the *Challenge* examines the many advances made as government, academia and the private sector responded to the "challenge" issued in 2006. It further delineates some of the complex issues that, five years later, have yet to be fully addressed. It acknowledges that the understanding of requirements has increased with experience while the advance of technology raises capabilities and expectations."



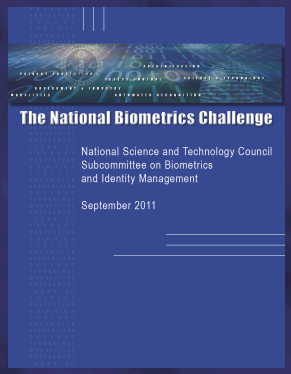
The challenge document update

- Considers the current state of the art
- Focuses on a fresh review of current requirements
- Identifies challenges to be met to address gaps

Update informed in part by

- The needs of the BIdM Subcommittee Organizations
- Recent Reports & Workshops (e.g. NAS, NSTIC, NSF)
- Targeted Meetings and Workshops

Targeted Meetings &Workshops



- **January 2011 Agency Meeting**
  - **BIdM Subcommittee**
- **February 2011 Industry Workshop**
  - **Hosted by IBIA**
- **May 2011 Workshop**
  - **Invited government, industry and academic participants**

BIdM Research & Development Working Group

No Significant Discussion of Privacy Issues

February 2011 IBIA Industry Workshop

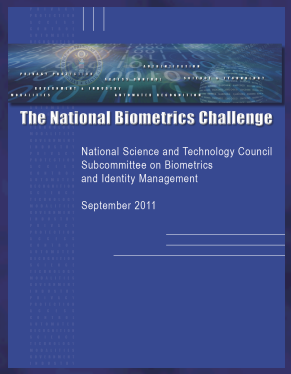
"Public perception, policy and law are the biggest challenges"
"Ensure that truth, rather than misinformation, is provided"
"Much more work on public outreach/messaging, guidelines, and best practice for Privacy is needed."
➔ General Agreement of industry participants a great deal more work was needed to clarify and solve privacy and civil liberty issues

May 2011 Invited Biometrics SME Workshop

➔ Professor Lisa Nelson an invited foundational speaker
➔ Four Scenarios Examined (Privacy etc. a concern in all four)

May 2011 Workshop Scenario Privacy Themes

- "Media hysteria towards the use of biometrics"
- "Paternalistic role of the USG with regards to biometric data and privacy stewardship"
- "Risks with the privacy of data"
- "Commercial and USG privacy concerns"
- "States have to stop passing legislation against the use"
- "Do we just wait 30 years for the next generation to be ok"
- Adapting to the use of biometrics seen as a generational issue
- "Public reservations keep biometrics from being widely implemented"
- "Protect your anonymity (or the perception of anonymity)"
- "Dissent in oppressive regimes (use of social media . . .)"
- "Develop privacy enabled biometrics"
- "People are more willing to give up anonymity for a greater security/ safety."
- "Public must feel comfortable and secure using biometrics and distinguish commercial use from USG use"



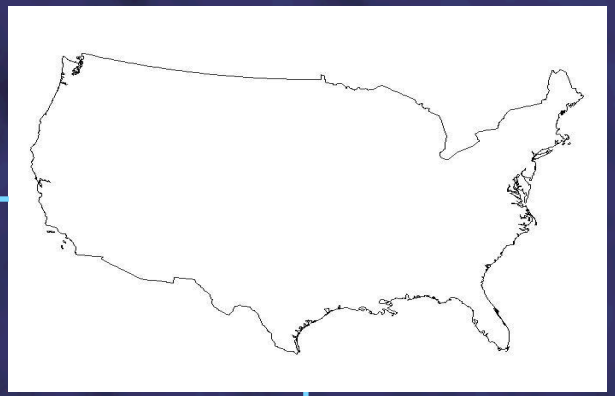
Selected Findings from *The National Biometrics Challenge 2011*

Advances, 2011 Environment, What Comes Next

Interoperability

FBI – IAFIS/NGI

US VISIT - IDENT



Interim Data Sharing
September 2006

Shared Services
October 2008

Visa Applicant Tenprint
Checks (via IDENT) 1/2008

Full Interoperability
December 2005

Two Finger Matching 2004

Shared Services Checks
(via IAFIS) 1/2012

DOD - ABIS

DOS - CCD

Technology

Basic and Applied Research:

- Biometric modality performance and robustness;
- New modalities;
- Multimodal and large-scale fusion;
- Quality assessments, enhancing quality;
- Tools, statistical methods and modeling frameworks;
- Study of socio-legal and business cases;
- Assessing vulnerabilities in biometric devices and systems;
- Fusion with results from related fields.

Education:

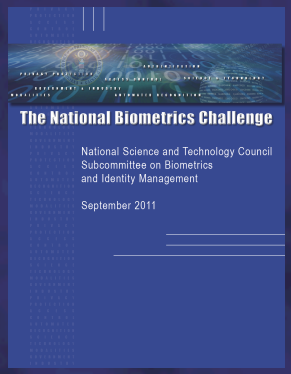
- Biometrics short courses – on campus, on site, web based;
- IEEE Certified Biometrics Professional program;
- University Associate and Bachelor level course offerings;
- An engineering –based Biometrics B.S. program;
- Doctoral and Master of Science training in Biometrics.

Fingerprint and Palmprint:

- Dramatic algorithm improvements to TMR @ 99% at FMR @ 10^{-3};
- Mobile capture devices for point-of-encounter identification;
- Latent background noise removal algorithm;
- low-quality ridge recognition algorithm;
- Open Source NFIQ 2.0 publication;
- FBI Appendix F extension to 1,000 PPI;
- Personal Identity Verification program and PIV-071006 specification .

Technology

(continued)



Face:

- Measured error rate dropping by half every two years;
- Faces in a crowd recognition;
- 3D face recognition;
- Video-to-video matching;
- Still-face-to-video matching;
- Proof-of-concept 100m face recognition with up to 10m/s motion;
- ANSI/NIST-ITL 1-2000 updated and replaced by ANSI/NIST-ITL 1-2011

Iris:

- Numerous algorithm providers, and algorithm advances, since circa 2005 patent expirations;
- Increased camera availability, lower failure to capture rates, faster capture time, lower cost;
- ANSI/NIST-ITL 1-2011 standardization

Voice:

- Advanced algorithms address cross-channel effects and speaker variants;
- Fast query and weighting algorithms that enable fusion;
- Devices specialized for clear capture while cancelling ambient background noise;
- Type 11 ANSI/NIST-ITL record

DNA Accepted as a Biometric

Mobile Multimodal Biometrics

2011 Biometric Environment

Primary Biometrics Uses Remain Law Enforcement, Border Control, and National Security:

- \+ Increased workload, accuracy, repository sizes with faster response times;
- \+ Commodity hardware and SOA allowed more flexible architecture & new capabilities;
- \+ Investment, policy changes and standardization produced greater interoperability;
- \+ Handheld, lower cost, capture devices permit point of interaction identification;
- \+ Impact of sample quality upon performance now widely understood and taken into account;
- \+ Very effective interagency coordination and partnering in place.
- – Need comprehensive architecture, standards, testing frameworks to exploit technology;
- – Potential of iris not fully realized pending CONOPS and methods for forensic analysis;
- – Potential of face recognition not fully realized pending PIE and aging algorithm advances;
- – Need better tools for non-ideal, non-cooperative, uncooperative presentation and acquisition;
- – Significant potential increases in volume and repository size may challenge systems.

2011 Biometric Environment

Limited Biometrics Adoption by Private Enterprise and for e-Government Services:

+ HSPD-12/FIPS 201 resulted in federal identity proofing and biometric credentialing;
+ Other countries, especially Japan and South Korea, widely adopting biometrics commercially;
+ Biometrically enabled Smartphone's are likely breakthrough technology for e-commerce;
+ UIDAI holds out potential to be transformational, driving policy and low cost.
– Framework for e-commerce identity proofing absent and an adoption barrier;
– FIPS 201 potential not fully realized at federal level, not realized outside government;
– Cost effective biometric capture devices at point-of-service absent for e-commerce;
– Framework for processing credential, authenticating identity, tying to transaction absent;
– Cost of replacing legacy identification processes, and uncertain cost/benefit a barrier;
– **Issues of privacy and anonymity remain to be addressed**.

User-Centric Technology Wave

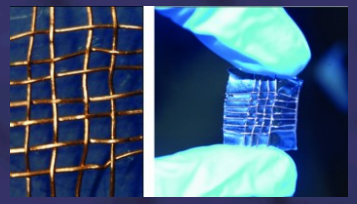
"Perhaps for the first time in the post-industrial, technology driven, information age, societies are not just reacting to technologies but shaping them on a global level."

- **"Rapidly increasing wireless connectivity and bandwidth coupled with cloud computing paradigms will render mobile devices as the preferred means to access services and interact with private and government entities."**
- **". . . this technological wave will inexorably raise civil and military users' expectations of government-sector biometric systems . . ."**
- **This commercial technological wave is expected to drive development and acceptance of biometric systems in commercial sector over the next 10 years**

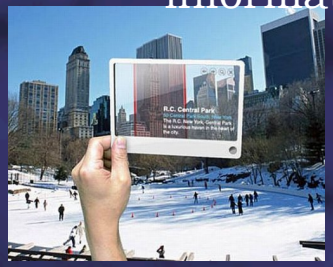
User-Centric Biometrics Approach

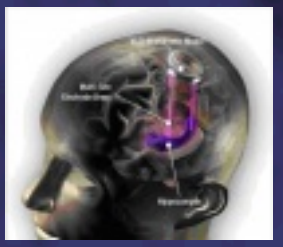
Personalized mobile information appliances

Global Cloud



Wearable and Biomimetic Systems





Customer Convenience and Value

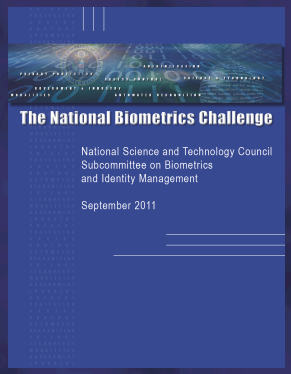
Privacy Policy

Last modified: March 1, 2012 (view archived versions)

Global Social Networks

Individual, Societal Behavior

Mobile applications requiring multi-factor authentication are expected to become commonplace



Privacy, Civil Rights, Civil Liberties and Anonymity Themes in 2011 Challenge

Privacy, Civil Rights, Civil Liberties and Anonymity - 2011

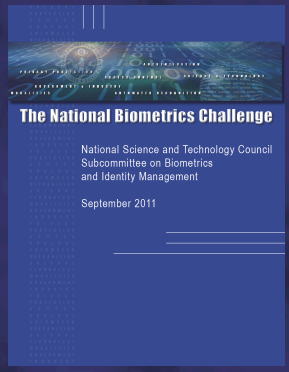
- "Facilitate the inclusion of privacy-protecting principles in biometrics system design" still part of purpose of Subcommittee
- "In America's free society, there are also social, legal, privacy and policy considerations in government and commercial programs related to automated identification and identity management.
- "The (2011) biometric environment is characterized by . . . current installations, on-going research, emerging technologies, institutional constraints, and privacy, civil rights, and civil liberties issues."
- "(for e-government and e-commerce) Privacy, civil rights and civil liberties are fundamental and highly complex issues that also need to be addressed as part of the entry process."
- "(in the commercial arena) The reluctance to adopt biometrics appears to be due to a combination of factors such as cost, institutional factors, authentication security concerns and privacy concerns."
- " . . . development and establishment of policies that address personal data ownership and use . . ."
- "a method for protecting biometric data in a renewable and revocable form must be developed."

Privacy, Civil Rights, Civil Liberties and Anonymity – 2011
(continued)

- "The benefits of biometric technology present both increased identity protection and risks to privacy, civil rights and civil liberties."
- 'To protect an individual's identity in this fast moving environment, technology and policies that protect the privacy, civil rights and civil liberties of individuals must advance at an equal pace."
- "The promise of new, groundbreaking applications of biometric technology cannot be realized without corresponding technology policies to protect privacy, civil rights and civil liberties."
- "Individuals . . . trust . . . use them in a manner that preserves anonymity when personally identifiable elements are not necessary."
- "It is the biometric collectors' responsibility to carefullydetermine the minimum biometric data necessary for each situation and to use the least invasive method."
- " . . . it is critical that researchers devote attention across the full range of biometric applications, including methods to use biometric technology to protect individual privacy, civil rights and civil liberties."

Privacy, Civil Rights, Civil Liberties and Anonymity – 2011
(continued)

- "While great strides can be witnessed in anonymization and de-identification research, more needs to be done in developing template protection (also known as cancelable or revocable biometrics)."
- "There are many instances when an individual has a legitimate expectation of anonymity and should not have to self identify. Therefore, biometric applications should enable people to emerge from anonymity to interact with a system for a specific service and then return to anonymity."
- "As the biometrics research community's ingenuity leads toward innovations, they must continually question how each new advance will affect privacy, civil rights and civil liberties."
- "Some individuals and organizations view biometrics as an invasive technology that systematically violates the individual's privacy. . . a concerted dialogue is needed . . . "



The 2011 National Biometrics Challenge reflects the objectives and priorities of the federal government Departments and their Components comprising the Biometrics and Identity Management Subcommittee. These are the federal agencies that operate the major national identification systems and direct the majority of federal RDT&E funding for Biometrics and Identity Management systems. The Subcommittee expects that the majority of federal funding over the next five years will address the priorities expressed in the *Challenge*.