The National Biometrics Challenge

National Science and Technology Council
Subcommittee on Biometrics

August 2006

Table of Contents

Page

About the National Science and Technology Council 1

About This Report 1

Executive Overview 2

The National Biometrics Challenge .

1. Introduction 3

2. Why Biometrics 4

3. The Primary Driving Forces. 5

   3.1 National Security 6
   3.2 Homeland Security and Law Enforcement 7
   3.3 Enterprise and E-Government (Electronic Government) Services 8
   3.4 Personal Information and Business Transactions 9

4. Communications and Privacy 10

5. Biometrics Challenges, Research Focus and Benefit 11

   5.1 Biometrics Sensors 12
   5.2 Biometrics Systems 13
   5.3 Biometrics Systems Interoperability 14
   5.4 Communications and Privacy 15

6. The Federal Government's Role in Biometrics Advancement 16

7. Summary 17

About the NSTC Subcommittee on Biometrics 18

Subcommittee on Biometrics 18

Department Leads 18
Biometrics Research Agenda ICP Team 19

Special Acknowledgements 19

Biometrics

A general term used alternatively to describe a characteristic or a process.

As a characteristic:
A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process:
Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Definitions used in this document are taken from the NSTC Subcommittee on Biometrics' Biometrics Glossary (http://www.biometrics.gov/referenceroom/docs/glossary.pdf)

About the National Science and Technology Council

The National Science and Technology Council (NSTC[1]) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the federal research and development enterprise. Chaired by the President, the NSTC is made up of the Vice President, the Director of the Office of Science & Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of 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. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals.

The purpose of the NSTC Subcommittee on Biometrics is to:

- Develop and implement multi-agency investment strategies that advance biometrics sciences to meet public and private needs;
- Coordinate biometrics-related activities that are of interagency importance;
- Facilitate the inclusion of privacy-protecting principles in biometrics system design;
- Ensure a 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 biometrics technologies.

About This Report

Government and industry have a common challenge in today's global society to provide more robust identity management tools and to deploy those tools intelligently to meet national and international needs. Collaboration among the biometrics community—government, industry and academia—on these common challenges is essential. To identify and partially address these issues, the NSTC chartered a Subcommittee on Biometrics.[2]

To identify key challenges in advancing biometrics development, the NSTC's Subcommittee on Biometrics has developed *The National Biometrics Challenge* based upon an 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. Electronic versions of this report and other Subcommittee documents are available at http://www.biometrics.gov.

[1] http://www.ostp.gov/nstc (accessed August 17, 2006)
[2] http://www.biometrics.gov (accessed August 17, 2006)

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.

Executive Overview

Government and industry have a common challenge in today's global society to provide more robust identity management tools, and identity governance principles on how to deploy these tools intelligently to meet national and international needs. Biometrics are the most definitive, real-time identity management tools currently available; however, use of the technology thus far has mainly consisted of systems designed to meet narrow objectives. To fully meet large-scale identity governance requirements, the use of biometrics technology must be made more robust, scalable and interoperable. Meeting these needs will require biometrics technology enhancements, adjustments of commercial business practices and system designs, and development of consensus on social, legal, privacy and policy considerations. Collaboration among the biometrics community—government, industry and academia—on these common challenges is essential.

The NSTC Subcommittee on Biometrics developed this report to describe the major challenges that must be addressed by the biometrics community. Working together to overcome these challenges, the community will meet evolving operational requirements while being supported by a robust biometrics industry.

The Subcommittee on Biometrics began its work by analyzing the community's four primary driving forces:

- National security;
- Homeland security and law enforcement;
- Enterprise and e-government services;
- Personal information and business transactions.

Consideration of these driving forces has led to the identification of four preeminent challenges:

- Improve collection devices—biometrics sensors;
- Develop more efficient and effective large-scale operational capabilities—biometrics systems;
- Establish standards for plug-and-play performance—biometrics systems interoperability;
- Enable informed debate on why, how and when biometrics should and can be used—biometrics communications and privacy.

Taking into account these driving forces and resultant biometrics challenges, this report highlights appropriate future roles for the federal government in advancing biometrics development to meet the needs of both our Nation and the broader worldwide community.

Recognition

A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply verification, closed-set identification or open-set identification (watchlist).

Verification

A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Identification

A task in which the biometric system searches a database for a reference matching a submitted biometric sample and, if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity.

The National Biometrics Challenge

1. Introduction

This report stems from the recognition of biometrics as a technology necessary to advance verification and identification of persons in four areas of national concern: national security, homeland security and law enforcement, enterprise and e-government services, and personal information and business transactions. As a result of these driving forces, a number of biometrics challenges have been identified regarding sensors, systems, interoperability and informed debate on the use of biometrics technology. Within each of these challenges are significant issues that the biometrics community must address to advance the technology and ensure it serves as a major asset for the Nation. This report, *The National Biometrics Challenge*, serves as a guiding document for the biometrics community in its pursuit of meaningful technological innovation.

Biometrics systems have been researched and tested for several years but have only recently entered into the public consciousness because of high-profile government deployments, exposure through entertainment and news media and growing use by consumers in day-to-day business transactions.

Many of the diverse undertakings of the government and commercial sectors require accurate and real-time recognition of individuals. Biometrics is an enabling technology that makes possible: tracking criminal histories and solving crimes, protecting wide-ranging border areas, screening individuals in high-volume transportation conduits and protecting automated consumer transactions. Current technologies are successful in specific implementations, but critical national needs require the evolution of biometrics technologies into open architecture systems for rapid, reliable and robust human identification and verification across a range of operational settings.

The federal government has served as a catalyst in the development of enterprise-wide biometrics systems for facility access, logical access and identity management. For example, the Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) provides automated fingerprint search capabilities, latent search capability, electronic image storage and electronic exchange of fingerprints and responses 24 hours a day, 365 days a year, in support of thousands of law enforcement organizations. This system, which contains biometrics records of more than 51 million criminal subjects, provides an "open-set" identification of submitted fingerprints, which

are checked against all known criminals in relevant portions of the database, normally within two hours of a criminal request and within 24 hours of civil fingerprint submissions. Each day, approximately 7,000 new records are added to the database.

This example demonstrates the power of biometrics and the added value that identity management systems offer. Current biometrics efforts have produced valuable first-step capabilities and opened opportunities for emerging technologies to revolutionize government and business practices. The federal government is uniquely positioned to continue to serve in the role of catalyst due to its various lines of business that are ideally suited to capitalize on advances in biometrics technology and its leadership roles in the standards community.

The missions of government and industry in today's global society demand more robust identity solutions that can be deployed on an increasingly large scale. The NSTC Subcommittee on Biometrics has developed this report to describe the major challenges that must be addressed by the biometrics community and to highlight the role of the federal government in fulfilling these requirements.

2. Why Biometrics

While biometrics serves as just one tool in a very large identity management toolbox, it is the most definitive real-time tool currently available. Because of its inherent association with a specific individual, biometrics can be layered with other tools (or in some cases replace them) to form more secure, easier to use verification solutions. The biometrics tool can also be used in identification applications to determine whether the collected biometrics are already associated with an individual.

Other identity management tools, such as passwords, personal identification numbers (PINs), tokens and cards, are in use today for applications ranging from employee verification to theme park access. Each of these tools has been used successfully for a variety of verification functions, but none can be used to recognize individuals definitively. Furthermore, traditional identity tools are more vulnerable to compromise, leading to potential system compromise or identity theft.[3] Biometric systems present an advantage over these other tools because they are based on an individual's physiological and behavioral characteristics, making them more difficult to steal, copy or compromise.

[3] "Since 2003, surveys have estimated the number of U.S. adults who became victims of identity theft within the preceding year at around 10 million, and the annual losses due to identity theft amount to $50 billion." http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html (accessed August 17, 2006)

US-VISIT

The US-VISIT program is the centerpiece of the United States government's efforts to transform our Nation's border management and immigration systems in a way that meets the needs and challenges of the 21st century. US-VISIT is part of a continuum of biometrically enhanced security measures that begins outside U.S. borders and continues through a visitor's arrival in and departure from the United States. From US-VISIT's inception in January 2004 through June 2006, DHS processed nearly 60 million travelers, stopping more than 1170 individuals at our ports of entry.

To achieve these effects, biometrics can either replace or work in combination with traditional identity management tools to form more secure, usable verification and identification solutions. Biometrics is the only tool that can be used by systems that require one distinct identity per person. Current U.S. examples include the FBI's IAFIS and Department of Homeland Security's (DHS') US-VISIT systems. In addition, some government benefit programs are beginning to employ biometrics technology in order to reduce fraudulent claims.

Overall, biometrics technologies offer enhanced security and convenience over traditional identity management tools in many verification applications and enable identification applications that would not otherwise be possible. However, while the technology has many merits, it also has a number of challenges that must be addressed before its use is to become widespread. The following sections articulate these challenges so that they may be addressed by the biometrics community.

3. The Primary Driving Forces

The NSTC Subcommittee on Biometrics recognizes that the future of the biometrics community will be shaped by four primary driving forces:

- National security (NS);
- Homeland security and law enforcement (HS/LE);
- Enterprise and e-government services (E);
- Personal information and business transactions (P).

These driving forces present four preeminent challenges for the biometrics community:

- Improve collection devices — biometrics sensors;
- Develop more efficient and effective large-scale operational capabilities — biometrics systems;
- Establish standards for plug-and-play performance — biometrics systems interoperability;
- Enable informed debate on why, how and when biometrics should be used — biometrics communications and privacy.

Analysis of each driving force reveals shared areas of concern, which in turn suggest the most crucial areas for enhanced emphasis and collaboration within the biometrics community. The following sections describe the needs of each driving force.

National Security

When the U.S. military rounded up suspected terrorists in a raid in Iraq in 2004, they booked and fingerprinted them using the same tools police in the U.S. use to check criminal backgrounds. The prints were logged, digitized, and sent to the FBI. Of the suspects apprehended in Iraq, 44 had criminal records in the U.S.

Based in part on successes such as this, the DoD created its own biometric database, the Automated Biometric Identification System (ABIS), which is modeled after, and co-located with, the FBI's IAFIS. Prints submitted to the DoD ABIS are also sifted through IAFIS. The value provided through these interoperable systems has been demonstrated several times. For example, suspected al Qaeda terrorist Mohamad al Kahtani was arrested in Southwest Asia in December of 2001, and was positively identified based on fingerprints taken when he was denied entry into the U.S. in August 2001 at Orlando International Airport.

3.1 National Security

3.1.1 Mission

The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity, as well as any previously used identities and past activities, over a geospatial continuum from sets of acquired data. Fusion and distribution of multi-modal biometrics and other contextual information can augment human interaction when a confrontation occurs with an unknown individual in a hostile or controlled setting. Depth of knowledge and real-time access to these data sets make biometrics a significant force multiplier and precision weapon in U.S. national security operations.

3.1.2 Needs

The defense and intelligence communities need capabilities that accurately recognize individuals and distinguish between those who pose a threat and those who do not in a wide range of operating conditions. These capabilities are needed to:

- Identify persons attributed to past or present illegal activities or those who pose future potential threats;
- Qualify and verify U.S. and non-U.S. trusted persons;

3.1.3 Applications

Key capacities for biometrics recognition systems include the capture and subsequent processing of many types of biometrics data:

- Live scan biometrics from persons of interest;
- Latent biometrics collected from various objects;
- Stand-off technologies to facilitate the collection of biometrics from a distance.

The defense and intelligence communities recognize the need to enable matching and searching capabilities for multiple biometrics modalities. The use of multiple biometrics requires increases in server capacity and techniques to reduce file size while maintaining data integrity and improvements in recognition algorithms. The defense and intelligence communities also require the ability to search against biometrics information collected or maintained by the Department of Defense (DoD), FBI, DHS, state and local law enforcement agencies, tribal law enforcement agencies and other sources as authorized by U.S. law and policy.

The Case For Biometrics at the Border

Each day DHS Customs and Border Protection (CBP) officers inspect more than 1.1 million passengers and pedestrians. In fiscal year 2005, over 84,000 individuals were apprehended at various ports of entry while trying to cross the border with fraudulent documents. On an average day, CBP intercepts more than 200 fraudulent documents, arrests over sixty people at ports of entry and refuses entry to hundreds of non-citizens, a few dozen of whom are criminal aliens attempting to enter the U.S. The number and types of documentation currently accepted is huge—over 8,000 different types—but the most popular forms of identification, a driver's license or birth certificate, are both prone to counterfeit and fraud and are easily obtainable by terrorists and other dangerous persons wishing to enter the U.S. illegally. Biometrics are now being used to combat this vulnerability.

3.2 Homeland Security and Law Enforcement

3.2.1 Mission

The homeland security and law enforcement communities require technologies to (1) secure the U.S. borders and (2) to identify criminals in the civilian law enforcement environment. At the same time, any solution must also seek to maintain international goodwill, ensure smooth passage of legitimate visitors and commerce, and provide surety in the identity and credentials of those given local or national trust.

3.2.2 Needs

The large numbers of agencies involved in the homeland security and law enforcement fields require biometrics devices that meet established standards and that improve interoperability and access to biometrics data across user communities. When participating agencies agree on standards, enterprise-wide solutions such as AFIS systems and first responder ID cards become possible. Agencies can then collaborate to efficiently and effectively implement common biometrics tools for use across geographic and departmental boundaries.

The homeland security and law enforcement communities have articulated a strong interest in multi-modal technologies and searches, reduced failure-to-enroll rates and affordable, rugged and portable devices. Driving these next-generation improvements are real-world experiences and assessments with variables such as the conditions at high-throughput border crossings and biometrics collections in hostile settings, as well as lessons learned from automated fingerprint identification systems and early efforts at enterprise-wide implementation of biometrics-enabled solutions.

3.2.3 Applications

Key applications in the homeland security and law enforcement communities include:

- Border management;
- AFIS interfaces for criminal and civil uses;
- First responder verification.

The homeland security and law enforcement communities recognize that some biometrics applications will be firmly anchored at the local level, with connectivity to regional and national systems. Biometrics would augment human interactions, provide accurate recognition and permit more accurate assessment and management of available data to ensure a single accurate identity across the entire homeland security and law enforcement enterprise.

The success of the FBI IAFIS system is due in large part to its standards-based connectivity to other systems. Fingerprints are acquired as a result of an arrest at the city, county, state or federal level. The fingerprints are processed locally and then electronically forwarded to a state or other federal agency system for processing. The fingerprints are then electronically forwarded through the CJIS Wide Area Network (WAN) to the FBI's IAFIS for processing.

As in the national security community, the homeland security and law enforcement communities similarly recognize the need for mobile, rugged and field-usable biometrics devices. Border patrol, first responder and law enforcement operations require that devices incorporate rugged components, communicability, and portability to work in austere environments even when basic services have been interrupted. Biometrics solutions must demonstrate long operational life as well as rapid and high-quality data capture and collection at stand-off ranges sufficient to ensure operator safety. In addition, biometrics solutions that incorporate real-time wireless communications connectivity to command centers can provide essential information for decision making.

3.3 Enterprise and E-Government (Electronic Government) Services

3.3.1 Mission

Enterprise solutions require the oversight of people, processes and technologies. Network infrastructures have become essential to functions of both business and government, and Web-based business models are now ubiquitous. As of January 2006, over one billion people use the Internet according, to Internet World Stats.[4] E-government services depend on this communications backbone. Consequently, securing access to these systems and ensuring one identity per user/end-user is essential. As enterprise information technology systems continue to grow in complexity and scale, identity management technologies and governance principles that enable authenticated users to be assigned appropriate levels of system access privileges will play an increasingly critical role in permitting transactions.

3.3.2 Needs

Currently, the best-known and most common identifiers are passwords. Multifactor recognition methods are often used to increase assurance. For example, an automatic teller machine (ATM) might require both an ATM card and a password or PIN to provide a higher level of assurance than is provided by either factor alone.

Next-generation concepts that streamline and secure recognition, as well as authorization and trust management technologies and tools, are needed to help mitigate potential vulnerabilities and increase scalability and interoperability. These solutions must be based upon open system biometrics standards and should enable their implementation to be consistent with privacy laws and widely accepted privacy principles.

[4] http://www.internetworldstats.com/stats.htm. (accessed July 6, 2006)

To counter the vulnerability of simple alphanumeric passwords, many organizations require the use of complex passwords containing a combination of numbers, letters and special characters. Depending on an organization's policy, passwords may need to be changed frequently or be unique to one system. These password management practices attempt to increase overall security but often come at a significant cost to individuals and organizations. Individuals may manage the difficulty of remembering many complicated passwords by writing them down on paper or in an electronic file. This practice negates overall system security. Forgotten passwords can significantly add to internal costs through an increased need for help desk staffing as well as lost productivity. Biometrics can simplify this user and infrastructure support problem by offering convenience (a biometric is always with you) and security (a biometric can be much more difficult to steal).

"Federated identity" is a capability that enables organizations to share trusted identities across the boundaries of their networks — with business partners, autonomous units and remote offices. Biometrics technologies support this capability by offering the prospect of implementing scalable identity management systems needed for cross-boundary trust management. However, there are continuing challenges in defining common recognition tools and, more importantly, in developing the forms of authorization that interdomain authentication will support.

Cross-agency collaboration, disaster and incident management for first responders, law enforcement data sharing, exchange of personnel records, and access to payroll records are all examples of government-to-government applications that could be performed through an online e-government portal. With 24 e-government initiatives[5] underway, authentication of users is a key security component to ensure and enable millions of safe, secure and trusted online transactions between governments, citizens and businesses. It is critical that an individual seeking access to sensitive information on behalf of one government entity be recognized, authorized and authenticated in order to attain access to appropriate information by another government entity. Equally important is the revocation of access privileges, which must be ubiquitously recognized among government activities.

3.3.3 Applications

Key application areas for biometrics in the enterprise and e-government services communities include:

- Identity verification within an organization;
- Identity verification across organizations.

The use of biometrics in information technology systems can reduce the identity governance burden for government organizations while providing government, citizen and business users with a secure and reliable authentication mechanism.

3.4 Personal Information and Business Transactions

3.4.1 Mission

Business institutions require business plans that meet customer demands for service at any time, from any location and through multiple communication devices, while safeguarding personal information and transaction data against unintended use. It is incumbent upon service providers to provide information only to the correct individuals. The use of biometrics is one of the most promising activities to counter the growing instances of identity theft.

[5] http://www.whitehouse.gov/omb/inforeg/e-gov/e-gov_benefits_report_2006.pdf (accessed August 17, 2006)

According to a Gartner report (G00129989, published July 28, 2005) hijacking of bank accounts was the most active form of financial fraud in the twelve months from May, 2004 to May, 2005. Based on the survey results of 5,000 on-line consumers, an estimated 3 million adults were victims of ATM/debit card abuse resulting in $2.75 billion in losses. Separately, an estimated 1.9 million adults were victims of illegal checking account transfers, resulting in nearly $3.5 billion in losses. According to the same Gartner survey, credit card fraud was still the most prevalent form of financial fraud with more than 3.9 million consumer victims, resulting in about $2.8 billion in losses.

3.4.2 Needs

Personal information and business transactions require fraud prevention solutions that increase security and are cost-effective and easy for customers to use. Businesses and individuals need to operate in the face of increasingly sophisticated fraud schemes such as “phishing”, “pharming” and other forms of identity theft attempts to illegally access individuals’ accounts or personal information.

3.4.3 Applications

Key application areas for personal information and business transactions include:

- Customer verification at physical point-of-sale;
- Online customer verification;
- Government benefits administration and licensing

Biometrics presented at transaction locations are used to differentiate authorized users from impersonators. Some applications where biometrics are expected to play an important role in verifying claimed identity during financial transactions include in-branch bank activities, ATM access, remote electronic access (telephone, Internet) and point-of-sale transactions.

The federal government is instituting programs for validating conformance to standards and performance of biometrics devices and systems for certain business applications (e.g., airport access control) that would also be useful for these industries.

4. Communications and Privacy

A fundamental understanding of biometrics technologies, applications and issues is required for various constituencies to competently discuss, and reach consensus on, where and how biometrics should be used. Achieving this consensus is necessary for the biometrics community to reach its potential as an automated identity management provider.

The biometrics community has produced excellent results in communicating the technical aspects of its contributions within the industry and among individual government organizations. A tipping point in the maturation of the technology has been reached, and now a *unified* message that stresses the utility, safety and convenience of biometrics, as well as the technical and operational issues, is necessary. Biometrics-based outreach activities flow through many channels and are heard by interested and disinterested constituencies that have varying degrees of familiarity with the subject matter. Multiple communications strategies must be developed and followed to reach the various major constituencies.

Privacy means more than "private" — it is not limited to keeping a secret. Most conceptions of secrecy assert that once the secret is revealed it is available for any public use (the individual "owner" of the secret loses all claims of control over the information). However, privacy claims can cover information and activities involving others (for example, bank accounts held by banks, medications known to doctors and pharmacists, etc.). In the biometric context, privacy protection governs the use of personal information that is shared (not "secret"). In response, the biometrics community must work to implement polices and processes that effectively govern the appropriate use of data, individually and in its aggregate. These policies and procedures should be clearly communicated to all affected constituencies.

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 on salient issues such as the safeguarding and sharing of biometrics data, and the constitutional protection of the availability of data to law enforcement in cases of criminal investigations. Formulation and subsequent widespread acceptance of privacy-protection policies for biometrics-based systems not only increases system acceptability but often improves system operation as well.

5. Biometrics Challenges, Research Focus and Benefit

Biometrics-enabled systems have shown their ability to identify imposters and criminals at border crossings and speed point-of-sale transactions while maintaining personal privacy and security. These successes have established a high expectation within the user community for biometrics systems that can do even more. The science upon which biometrics is based has the capacity to deliver additional improvements for the community.

Significant progress is required for the U.S. to realize fundamental improvements across all biometrics modalities and their systems and thereby enable more advanced operational systems. An analysis of common needs within the driving forces identified four main challenges—biometrics sensors, biometrics systems, biometrics systems interoperability and communications and privacy—each of which is described with three subsections:

- Description of challenge: A summary of high-priority needs in multiple driving forces; intended to stimulate and direct multi-disciplinary thinking;
- Focus of research: Recommended near-term research to meet high-priority needs; intended to focus and direct researchers to solve problems of need;
- Benefits: Description of anticipated end-state enhancements; intended to explain the benefits of successful research.

Successful pursuit of these biometrics challenges will generate significant advances in capabilities designed to improve safety and security in future missions within national and homeland security, law enforcement, and personal information and business transactions.

- **NS: National Security**
- **HS/LE: Homeland Security and Law Enforcement**
- **E: Enterprise and E-Government Services**
- **P: Personal Information and Business Transactions**

Cooperative User

An individual that willingly provides his/her biometric to the biometric system for capture. Example: A worker submits his/her biometric to clock in and out of work.

Non-cooperative User

An individual who is not aware that his/her biometric sample is being collected. Example: A traveler passing through a security line at an airport is unaware that a camera is capturing his/her face image.

Uncooperative User

An individual who actively tries to deny the capture of his/her biometric data. Example: A detainee mutilates his/her finger upon capture to prevent the recognition of his/her identity via fingerprint.

5.1 Biometrics Sensors

Description of Challenge

- Rapid collection of face, finger and iris data in mobile and harsh environments that meet technical, safety and quality standards, thus enabling immediate submission to national-level biometrics screening systems (NS, HS/LE)
- Quality collection of biometric data of non-cooperative users at distances (NS, HS/LE)
- Quality collection of biometrics data in relaxed conditions (NS, HS/LE)
- Biometrics templates that can be revoked and replaced to uniquely represent the source individual should that individual's template become compromised (NS, HS, E, P)
- Next generation sensors (NS, HS, E, P)

Focus for Biometrics Research

- Biometric sensors that automatically recognize the operating environment (such as outdoor/indoor/ambient lighting or changing backgrounds) and communicate with other system components to automatically adjust settings to deliver optimal data
- Rapid, intuitive collection (less than 15 seconds) of rolled-equivalent fingerprints from cooperative users
- Biometric sensors that:
  - Have virtually no failures-to-enroll
  - Are low cost
  - Are easy to use (intuitive to end-users)
  - Provide standards-based data
  - Can be integrated into existing systems easily
  - Incorporate liveness detection
  - Are rugged (varying operating temperatures, waterproof and UV-resistant)
- Contactless and/or self-sterilizing contact fingerprint sensors
- Biometric sensors that can collect standards-quality imagery from a distance
- Middleware techniques/standards that will permit "plug-and-play" capability of biometrics sensors
- 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
- Means to transform an individual's biometrics template at time of capture such that the transformed template would be suitable for enrollment and matching, but revocable and replaceable should it become compromised

The public appears to be ready to embrace biometrics as a form of strong authentication for financial transactions. An international survey*, commissioned by Unisys Corporation and published in February, 2006 concluded that:

- **Two-thirds (66%) of banking consumers worldwide worry about identity fraud and the safety of their bank and credit card accounts.**
- **Almost half (45%) of bank account holders worldwide are willing to switch banks for better protections from identity fraud.**
- **More than one-third of worldwide consumers are willing to pay additional bank fees for better security protection.**
- **The U.S leads in ID fraud instances (17% of U.S. consumers cite they have been victims) followed by the U.K. (11%), Brazil (9%), Mexico (8%), France (8%), Australia (7%), Germany (3%) and Hong Kong (1%).**
- **Biometrics e.g., iris or fingerprint scans) is the preferred method cited by consumers to fight fraud and identity theft, followed by smart cards, tokens, and more passwords.**

*** Unisys, Inc. 2005, http://www.unisys.com/eprise/main/admin/micro/doc/ID_Fraud_Pg Prep.qxt.pdf**

Benefits

- Rapid collection of biometrics data in uncontrolled situations that can be compared against, and added to, data in national-level screening systems in an accurate, rapid, safe and easy manner
- Real-time comparison of first-time foreign visitors to terrorist/criminal databases
- Single identity for individuals across the entire law enforcement enterprise (field, police station, court, jail, etc.)
- Fiscal viability of biometrics in enterprise-security and financial transactions
- System capabilities unaffected if a change in sensor becomes necessary
- Biometrics templates that protect against biometrics identity theft by permitting stolen templates to be revoked and replacement templates to be enrolled without degrading system performance

5.2 Biometrics Systems

Description of Challenge

- Consistently high recognition accuracy under a variety of operational environments (NS, HS/LE, E, P)
- Ability to determine which components are most appropriate for a given application (NS, HS/LE, E, P)
- Intuitive interfaces for operators and end-users (NS, HS/LE, E, P)
- Remote, unattended enrollment and recognition of end-users with varying sensors (E, P)
- Return on investment (ROI) models for various applications to aide in determining the efficacy of incorporating biometrics (NS, HS, E, P)

Focus for Biometrics Research

- 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 biometrics 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

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

5.3 Biometrics Systems Interoperability

- **NS: National Security**
- **HS/LE: Homeland Security and Law Enforcement**
- **E: Enterprise and E-Government Services**
- **P: Personal Information and Business Transactions**

Description of Challenge

- Ability to easily/rapidly/seamlessly integrate system components into functioning systems and then swap components as needed without losing functionality (NS, HS/LE, E)
- Validate and verify the authenticity and use restrictions of data collected from multiple sources (NS, HS/LE)
- Develop secure and verifiable means for protecting collected data for its lifetime (NS, HS/LE, E, P)
- Build an understanding of enterprise-wide implementations across a multitude of constituencies (NS, HS/LE, E, P)

Focus of Research

- Open standards:
  - Biometrics data interchange formats
  - File frameworks
  - Application interfaces
  - Implementation agreements
  - Testing methodology
- Conformance and interoperability testing for standards
- Adoption of standards-based solutions
- Common metadata structures and associations with biometrics data

- NS: National Security
- HS/LE: Homeland Security and Law Enforcement
- E: Enterprise and E-Government Services
- P: Personal Information and Business Transactions

The NSTC Subcommittee on Biometrics' *Privacy & Biometrics: Building a Conceptual Foundation,* seeks to connect privacy and biometrics at a structural level so that both fields can be understood within a common framework. The paper provides a general overview of both privacy and biometrics and offers a perspective through which to view the convergence of both.

- Guidelines for auditing biometrics systems and records
- Framework for integration of privacy principles in biometrics system design

Benefits

- Real-time, controlled and documented data sharing between biometrics systems
- Consistent enterprise-wide performance across different user groups and organizations
- Integration of disparate systems produced by different vendors
- Eradication of non-operability caused by proprietary middleware, hardware and software

5.4 Communications and Privacy

Description of Challenge

- Fundamental understanding of biometrics technologies, operational requirements and privacy principles to enable beneficial public debate on where and how biometrics systems should be used (NS, HS/LE, E, P)
- Embed privacy functionality into every layer of the architecture, from the sensor through the system to the interoperable biometrics network (NS, HS/LE, E, P)
- Privacy-protective solutions that meet operational needs, enhance public confidence in biometrics technology and safeguard personal information (NS, HS, E, P)

Focus of Research

- Develop a consistent, accurate and understandable message across the biometrics community
  - Canvass opinion leaders—first adopters, commercial deployers, educational users, media business/technology columnists and everyday consumers
  - Develop easy-to-understand informational literature for universal reference
  - Establish a speakers' bureau and subject matter-expert cadre trained in media relations
  - Quickly respond to high-profile issues
- Engage in proactive outreach when designing systems and policies
  - Clearly articulate the operational purpose of proposed systems, the underlying authority of the organization and the specific authority for the system
  - Engage the judicial, legislative and executive branches of affected local, state and federal governments

Multiple federal agencies collaborated to issue a request for information (RFI) in September 2005 for a fast-capture fingerprint device. The RFI described performance and size specifications that were more rigid than currently available capture devices but better represented the operational needs of agencies throughout the federal government in a single specification. Initial responses were that it would take years to develop such a device. Manufacturers soon recognized, however, that they would be better served devoting their research energies to meeting this one requirement than seeking solutions to multiple, unspecified requirements for individual application areas. One manufacturer was able to produce a device and received FBI certification in March 2006; a few hundred units were ordered that very day. The NSTC Subcommittee on Biometrics expects additional manufacturers to provide certified devices soon.

    - Embrace concerned opposition and seek their input
    - Communicate, in the appropriate form, the results of privacy assessments to demonstrate the practice and value of transparency in the use of personal information
- Study how best to relay information and/or facilitate discussion with varying groups
- Create enhanced guidelines and informative examples of integrating privacy and biometrics technology
- Develop best practices for operating biometrics systems and interfacing with end-users

Benefits

- A scientifically educated and aware public that can serve as a partner in making appropriate decisions about the nation's biometrics investments, guiding their adoption and debating the societal implications of biometrics systems
- Goodwill among various constituencies
- The demystification of biometrics technologies and their fundamental operations
- Deployments appropriate to the scale and purpose of the intended applications

6. The Federal Government's Role in Biometrics Advancement

The National Biometrics Challenge recognizes the operational importance of biometrics and its potential to significantly improve the security and prosperity of our Nation. This report identifies the key technical and planning challenges that the entire biometrics community must address for this vision to become reality. The role of the federal government in meeting these challenges is limited, yet significant. In general, and as outlined in "Science for the 21st Century"[6], the four major responsibilities of the federal science enterprise are to:

1. Promote discovery and sustain the excellence of the Nation's scientific research enterprise;
2. Respond to the Nation's challenges with timely, innovative approaches;
3. Invest in and accelerate the transformation of science into national benefits;
4. Achieve excellence in science and technology education and in workforce development.

Keeping these four overarching responsibilities in mind, the NSTC Subcommittee on Biometrics identified the following roles for

[6] http://www.ostp.gov/nstc/21stCentury/Final_sm.pdf (accessed August 17, 2006)

The US Government has developed three sister websites to assist the community's outreach efforts:

- **Biometrics.gov – The US Government's central location to find information about biometrics and related federal programs;**
- **Biometricscatalog.org – A "catalog" of publicly-available biometrics-related information that is kept up to date by its users;**
- **Biometrics.org – Information on Biometric Consortium activities, including the Biometric Consortium Conference and BC Bulletin Board.**

the government to take in implementing *The National Biometrics Challenge*:

- Assist in the identification of priority cross-community needs for biometrics;
- Invest in cutting-edge basic research that produces new discoveries that can advance biometrics and other technologies in the future;
- Describe government needs in as specific terms as possible so that industry and academia can devote resources to solving real problems;
- Where appropriate, provide resources and/or guidance to overcome those obstacles that the community is unable to provide on its own;
- Maximize efficiency and effectiveness of the federal research, development, testing and evaluation enterprise by:
  - Planning biometrics activities across the federal government to meet interagency needs;
  - Selecting activities through competitive, peer-reviewed award and review processes;
  - Ensuring activities meet scientific and privacy-rights standards;
- Participate in biometrics open standards development, standards adoption, conformance test tool development, conformity assessment system development, and harmonization of biometrics, security and authentication standards;
- In support of first, second and third-party testing, perform testing and evaluation for biometrics performance, interoperability, collection and maintenance of data, and development of large databases;
- Assist in the promotion of a scientifically literate population and a supply of qualified technical personnel commensurate with national needs;
- Strengthen international partnerships in order to foster the advancement and standardization of biometrics technologies.

7. Summary

The nascent biometrics community successfully faced a difficult challenge five years ago as it was called upon to meet urgent homeland and national security needs. The community's past success, however, has created greater challenges, as government and industry are more dependent than ever on more robust identity management tools and identity governance principles. *The National Biometrics Challenge* identifies these key challenges and the role of government in meeting them. Working together in the future, as in the past, will enable the biometrics community to meet these new

The NSTC Subcommittee on Biometrics has produced a suite of introductory documents on biometrics. These documents will serve as the foundation of the subcommittee's future strategic outreach plans. The subcommittee highly encourages others in the biometrics community to use them so that the biometrics community as a whole benefits from having a consistent message and a source of reference material. The suite consists of documents in three areas:

- **Basic Introduction**
- **Technologies**
- **Cross-Cutting Topics**

challenges, and produce a robust, vibrant, biometrics community that is able to provide systems and services for years to come.

About the NSTC Subcommittee on Biometrics

The NSTC Subcommittee on Biometrics serves as part of the internal deliberative process of the NSTC. Reporting to and directed by the Committee on Homeland & National Security and the Committee on Technology, the Subcommittee:

- Develops and implements multi-agency investment strategies that advance biometrics sciences to meet public and private needs;
- Coordinates biometrics-related activities that are of interagency importance;
- Facilitates the inclusions of privacy-protecting principles in biometrics system design;
- Ensures a 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 biometrics technologies.

Subcommittee on Biometrics

Co-chair: Duane Blackburn (OSTP)
Co-chair: Chris Miles (DOJ)
Co-chair: Brad Wing (DHS)
Executive Secretary: Kim Shepard (FBI Contractor)

Department Leads

Mr. Jon Atkins (DOS)
Dr. Sankar Basu (NSF)
Mr. Duane Blackburn (EOP)
Ms. Zaida Candelario (Treasury)
Dr. Joseph Guzman (DoD)
Dr. Martin Herman (DOC)
Ms. Usha Karne (SSA)
Dr. Michael King (IC)
Mr. Chris Miles (DOJ)
Mr. David Temoshok (GSA)
Mr. Brad Wing (DHS)
Mr. Jim Zok (DOT)

Biometrics Research Agenda Interagency Coordination Plan (ICP) Team

Champions: Mike Hogan (NIST)
Stephen Dennis (DHS S&T)

ICP Members & Support Staff:

Dr. Sankar Basu (NSF)
Mr. Duane Blackburn (OSTP)
Dr. Bert Coursey (DHS S&T)
Dr. Joseph Guzman (DoD)
Dr. Joe Kielman (DHS S&T)
Dr. Michael King (ITIC)
Mr. Chris Miles (DOJ)
Mr. Brad Wing (DHS US-VISIT)
Mr. Jim Zok (DOT)

Special Acknowledgements

The Research Agenda ICP Team wishes to thank the following contributors for their assistance in developing *The National Biometrics Challenge*:

- Mike Hogan, Duane Blackburn, Jim Zok, and Stephen Dennis for performing primary author tasks.
- Kate Crawford, Chang Chang, and Ken McMurrain, BRTRC, for editorial and graphical assistance.
- International Biometric Industry Association and International Biometric Group for their assistance in understanding business needs/issues for biometrics.

www.biometrics.gov