National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Biometrics Standards

Introduction

Standards for the collection, storage, and sharing of biometric data are of utmost importance to government and private systems. This paper provides an entry-level understanding of how biometric standards are developed and the current status of biometric standards by answering the following questions:

- What are biometric standards?
- Why are biometric standards important?
- What types of biometric standards are there?
- Who develops standards?
- How are standards developed?
- What is conformity assessment?
- Is the use of biometric standards mandatory or optional?
- Where do I find more information about a specific standard?

What are biometric standards?

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Guide 2:2004 defines a standard as "a document, established by consensus that provides rules, guidelines or characteristics for activities or their results." [1] The Biometric Consortium website defines standards as "a general set of rules to which all complying procedures, products or research must adhere." [2]

Standards play a role in everyday life by establishing the size, configuration, or protocol of a product, process, or system. Standards specify performance of products or personnel and also define terms so that there is no misunderstanding among those using the standards.

As examples, standards help ensure that film to fit 35mm cameras can be purchased anywhere in the world, that a light bulb fits a socket, and that plugs for electrical appliances fit outlets. With design and performance standards, homes, workplaces and public buildings are safer from collapse, fire and explosion.[3]

For any given technology, standards assure the availability of multiple sources for comparable products and of competitively-

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

priced products in the marketplace. Standards support the expansion of the marketplace.[4]

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process, a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.[5]

Biometric standards specify:

- formats for the interchange of biometric data;
- common file formats that provide platform independence and separation of transfer syntax from content definition;
- application program interfaces and application profiles;
- performance metric definitions and calculations;
- approaches to test performance; and
- requirements for reporting the results of performance tests.

Why are biometric standards important?

Standards enable development of integrated, scalable, and robust solutions and reduce the cost of development and maintenance of system solutions. Biometric standards have been and are currently being developed on both the national and international levels. These efforts are focusing on creating a standard set of biometric data interchange definitions, developing standards to promote interoperability between various systems, and creating standards for testing biometrics and for testing conformance to biometric standards. Standards should be technology neutral and not favor any particular vendor or modality.[5]

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

What types of biometric standards are there?

Biometric standards include, but are not limited to:[6]

- Technical Interfaces — specify interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems; and specify the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their applications. Examples include ANSI INCITS 358-2002 BioAPI Specification v1.1 and ANSI INCITS 398-2005 [NISTIR 6529-A] Common Biometric Exchange File Format (CBEFF).
- Data Interchange Formats — specify the content, meaning, and representation of formats for the interchange of biometric data, e.g., Finger Pattern Based Interchange Format, Finger Minutiae Format for Data Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format, Finger Image Based Interchange Format, Signature/Sign Image Based Interchange Format, and Hand Geometry Interchange Format; and specify notation and transfer formats that provide platform independence and separation of transfer syntax from content definition. Examples include ANSI INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange, and ANSI INCITS 379-2004 Iris Image Interchange Format.
- Application Profile Standards — specify one or more base standards and standardized profiles, and where applicable, the identification of chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function. Examples include ANSI INCITS 383-2003 Biometrics-Based Verification and Identification of Transportation Workers, and ANSI INCITS 394-2004 Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management.
- Performance Testing and Reporting — specify biometric performance metric definitions and calculations,

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

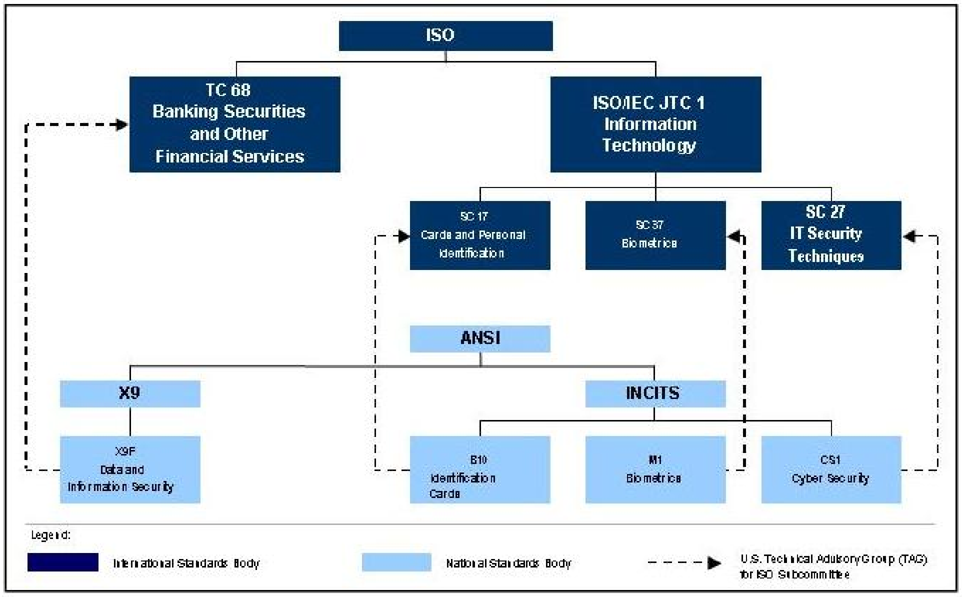
approaches to test performance, and requirements for reporting the results of these tests. Examples include ANSI INCITS 409.1-2005 Biometric Performance Testing and Reporting Part 1 - Principles Framework; ANSI INCITS 409.2-2005 Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology; and ANSI INCITS 409.3-2005 Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies.

Who develops standards?

The government agencies and Standards Development Organizations (SDOs) who develop biometric standards include:

- National Institute of Standards and Technology
- InterNational Committee for Information Technology Standards (INCITS) M1
- Joint Technical Committee 1 (JTC 1)/Subcommittee 37 (SC 37)
- Organization for the Advancement of Structured Information Standards (OASIS)

Each of the following subsections provides a brief description of each SDO.


ISO
TC 68 Banking Securities and Other Financial Services
ISO/IEC JTC 1 Information Technology
SC 17 Cards and Personal Identification
SC 37 Biometrics
SC 27 IT Security Techniques
ANSI
X9
INCITS
X9F Data and Information Security
B10 Identification Cards
M1 Biometrics
CS1 Cyber Security
Legend:
International Standards Body
National Standards Body
U.S. Technical Advisory Group (TAG) for ISO Subcommittee

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

INCITS M1

INCITS is accredited by and operates under rules approved by the American National Standards Institute (ANSI). INCITS is the primary US focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. INCITS also serves as ANSI's Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1 (JTC 1), which is responsible for international standardization in the field of Information Technology.

In November 2001, INCITS established M1 with membership open to any organization (e.g., academic institutions, federal agencies, companies) directly and materially affected by M1 activities. As the US TAG to SC 37, INCITS M1 is responsible for establishing US positions and contributions to SC 37, as well as representing the US at SC 37 meetings. M1 presently has five standing task groups:

- M1.2 Biometric Technical Interfaces — develops standards for interfaces and interactions between biometric system components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems.
- M1.3 Biometric Data Interchange Formats — develops standards for the content, meaning, and representation of biometric data interchange formats.
- M1.4 Biometric Profiles — develops profile standards to ensure the interoperability of biometric information in specific applications (e.g., Biometric Based Verification and Identification of Transportation Workers, Border Management, Point of Sale).
- M1.5 Biometric Performance Testing and Reporting — develops standards for biometric performance metric definitions and calculations, and approaches to test performance and requirements for reporting the results of these tests.
- M1.6 Societal Aspects of Biometric Implementations — develops technical reports that address the study and standardization of technical solutions to cross-jurisdictional and societal aspects of biometric implementations.

In addition to the standing task groups, M1 has the ability to form Ad Hoc Groups to perform a specific task and report back to the

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

parent body, e.g. M1 or M1.3. Upon completion of its report, or at the second meeting of the parent body following the Ad Hoc Group's establishment, the Ad Hoc Group is dissolved unless there is sufficient reason to extend its duration. Examples include the Ad Hoc Group on Data Quality (QUAHOG), the Ad Hoc Group on the Use of BioAPI to Support Ten-print Capture (AHGUBSTC), the Ad Hoc Group on Round Robin Testing (AHGRRT), and the Ad Hoc Group on INCITS 378 Encoding Rules (AHGIER). Since an Ad Hoc Group is limited in duration and scope, its business may be conducted less formally than that of any other INCITS Organizational Entity (IOE), so the documentation of its report serves as principal record of the group.

National Institute of Standards and Technology (NIST)

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by NIST for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use Government-wide. In addition to being the nation’s premier measurement research laboratory, NIST develops FIPS when there are compelling Federal Government requirements such as for security and interoperability for which no acceptable industry standards or solutions exist. FIPS do not apply to national security systems. Other documents published by NIST include NIST Interagency Reports (NISTIR) and NIST Special Publications. Examples of these are NISTIR 6529-A, “Common Biometric Exchange Formats Framework (CBEFF) ” and NIST Special Publication SP 500-245, “ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information,” respectively.

JTC 1/SC 37

JTC 1/SC 37 is responsible for the international standardization projects for generic biometric technologies to support data interchange, interoperability, and testing. Established in June 2002 by JTC 1, SC 37 has twenty-one participating member countries, six observer countries, and eleven liaison organizations. As with INCITS M1, SC 37 has maintained fast-paced development activities since its inception, due to the increased demand for proven biometric technologies. To manage these efforts, SC 37 has also organized a number of Working Groups (WGs) that closely align with the M1 Task Groups:

- WG1 Harmonized Biometric Vocabulary — develops standardized definitions for biometric vocabulary terms.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

- WG2 Biometric Technical Interfaces — develops international standards for BioAPI and CBEFF, as well as a number of other related projects.
- WG3 Biometric Data Interchange Formats — develops international versions of the biometric data interchange format standards.
- WG4 Biometric Functional Architecture and Related Profiles — develops international biometric profile standards to support biometric interoperability for applications.
- WG5 Biometric Testing and Reporting — develops international standards for biometric performance testing and reporting.
- WG6 Cross-jurisdictional and Societal Aspects — currently developing an international technical report on privacy concerns and other social concerns related to biometric standards.

OASIS

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces Web services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.[7]

OASIS XML Common Biometric Format (XCBF) provides a standard way to describe information that verifies identity based on human characteristics such as DNA, fingerprints, iris scans, and hand geometry. The OASIS XCBF Technical Committee defined a common set of secure XML encodings for the patron formats specified in the Common Biometric Exchange File Format (CBEFF) (NISTIR 6529). These XML encodings are based on the ASN.1 schema defined in ANSI X9.84:2003 Biometrics Information Management and Security. They conform to the XML Encoding Rules (XER) for ASN.1 defined in ITU-T Recommendation X.693, and rely on the security and processing requirements specified in X9.96 XML Cryptographic Message Syntax (XCMS).[7]

Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity,

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.[7]

How are standards developed?

Consensus standards are commonly developed using a process that proceeds from a project proposal to the cyclic writing, editing, and commenting of the Draft Standard, which, upon approval by the member bodies, culminates in the Published Standard. The following outlines one such possible process:

- Project Proposal
- Draft Standard
  - Working Draft
  - Committee Draft
  - Final Draft
- Member Body Approval
- Published Standard

Successive drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is circulated to all member bodies for voting and comments within a period set by the SDO. If the approval criteria, which vary from SDO to SDO and can range from a simple majority of members voting to other more complex criteria, are not met, the Draft Standard is returned for further study and a revised Draft Standard will again be circulated for voting and comments. Most SDOs review their standards at specified time intervals, to determine whether a given standard should be confirmed, revised, or withdrawn.

If a document with a certain degree of maturity is available at the start of a standardization project, for example a standard developed by another organization, it is possible to omit certain stages of the process. In a so-called “fast-track procedure,” a document is submitted directly to the member bodies for approval as a draft standard without passing through the previous stages.[8]

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

What is conformity assessment?

ISO/IEC Guide 2:1996 defines conformity assessment as “any activity concerned with determining directly or indirectly that relevant requirements are fulfilled”.[3] Conformity assessment of a product to a given standard raises the user’s assurance that the product will perform in the manner expected with regard to the intent of the written specification.

While a standard is a technical expression of how to make a product safe, efficient, and compatible with others, a standard alone cannot guarantee performance. Conformity assessment, however, provides assurance to users by increasing consumer confidence when personnel, products, systems, processes, or services are evaluated against the requirements of a standard.[3]

The development of conformance tools makes possible the establishment of conformity assessment programs to validate conformance, e.g., to ANSI INCITS 358-2002 BioAPI Specification v1.1, and to support development of products conforming to voluntary consensus biometric standards. By making the tools available, developers may use these same test tools to ensure standards conformance before products are released.

Is the use of biometric standards mandatory?

In general, standards usage is optional. However, the real benefits of standards are realized by organizations that require the application and use of standards. Some organizations maintain a registry or database of standards that must be applied in acquiring, developing, and maintaining systems. These organizations will not purchase products or services that do not conform to such required standards.

Where do I find more information about a specific standard?

An excellent starting point for more information about a specific standard is the websites of organizations that help develop the standard, e.g., http://www.iso.org, http://www.ansi.org, http://www.nist.gov, etc. There are also additional online resources available such as NSSN: A National Resource for Global Standards (http://www.nssn.org/search.html) and the World

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Standards Services Network (http://www.wssn.net/WSSN/index.html).

Document References

[1] ISO/IEC Guide 2:2004 <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39976&ICS1=1&ICS2=120&ICS3=>.

[2] The Biometric Consortium, "Standards Activities," <http://www.biometrics.org/html/standards.html>.

[3] American National Standards Institute, "Frequently Asked Questions," <http://www.ansi.org/about_ansi/faqs/faqs.aspx?menuid=1>.

[4] National Institute of Standards and Technology – Information Technology Laboratory, "Biometrics Standards and Current Standard-Related Activities" 18 February 2002 (updated 8 January 2003) <http://www.itl.nist.gov/div893/biometrics/standards.html>.

[5] National Science & Technology Council Subcommittee on Biometrics, "Frequently Asked Questions" 16 August 2005 <http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf>.

[6] InterNational Committee for Information Technology Standards, "M1 - Biometrics" <http://www.ncits.org/tc_home/m1.htm>.

[7] Organization for the Advancement of Structured Information Standards <http://www.oasis-open.org/>.

[8] International Organization for Standardization, "Stages of the development of International Standards" 30 September 2003 <http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/proc/proc.html>.

Standards Glossary

AHGIER	Ad Hoc Group on INCITS 378 Encoding Rules
AHGRRT	Ad Hoc Group on Round Robin Testing
AHGUBSTC	Ad Hoc Group on the Use of BioAPI to Support Ten-print Capture
ANSI	American National Standards Institute
CBEFF	Common Biometric Exchange File Format

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

FIPS	Federal Information Processing Standards
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
IOE	INCITS Organizational Entity
ISO	International Organization for Standardization
JTC 1/SC 37	Joint Technical Committee 1/Subcommittee 37
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Reports
OASIS	Organization for the Advancement of Structured Information Standards
QUAHOG	Ad Hoc Group on Data Quality
SAML	Security Assertion Markup Language
SDO	Standards Development Organizations
SMT	Scar Mark & Tattoo
TAG	Technical Advisory Group
WG	Working Group
XCBF	XML Common Biometric Format
XCMS	XML Cryptographic Message Syntax
XER	XML Encoding Rules

About the National Science and Technology Council

The National Science and Technology Council (NSTC) 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 membership of the NSTC is made up of the Vice President, the Director of the Office of Science and 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

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

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 work of the NSTC is organized under four primary committees; Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees a number of sub-committees and interagency working groups focused on different aspects of science and technology and working to coordinate the various agencies across the federal government. Additional information is available at www.ostp.gov/nstc.

About the 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 biometric sciences to meet public and private needs;
- Coordinates biometrics-related activities that are of interagency importance;
- Facilitates the inclusions of privacy-protecting principles in biometric 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 biometric technologies.

Additional information on the Subcommittee is available at www.biometrics.gov.

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

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)

Communications ICP Team

Champion: Kimberly Weissman (DHS US-VISIT)

Members & Support Staff:

Mr. Richard Bailey (NSA Contractor)
Mr. Duane Blackburn (OSTP)
Mr. Jeffrey Dunn (NSA)
Ms. Valerie Lively (DHS S&T)
Mr. John Mayer-Splain (DHS US-VISIT Contractor)
Ms. Susan Sexton (FAA)
Ms. Kim Shepard (FBI Contractor)
Mr. Scott Swann (FBI)
Mr. Brad Wing (DHS US-VISIT)
Mr. David Young (FAA)
Mr. Jim Zok (DOT)

National Science and Technology Council (NSTC)
Committee on Technology
Committee on Homeland and National Security
Subcommittee on Biometrics
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

Special Acknowledgements

The Communications ICP Team wishes to thank the following external contributors for their assistance in developing this document:

- John Mayer-Splain, DHS/US-VISIT, for performing background research and writing the first draft
- Mike Hogan, Dave Lohman, and the Standards ICP Team for reviewing the document and providing numerous helpful comments

Document Source

This document, and others developed by the NSTC Subcommittee on Biometrics, can be found at www.biometrics.gov.