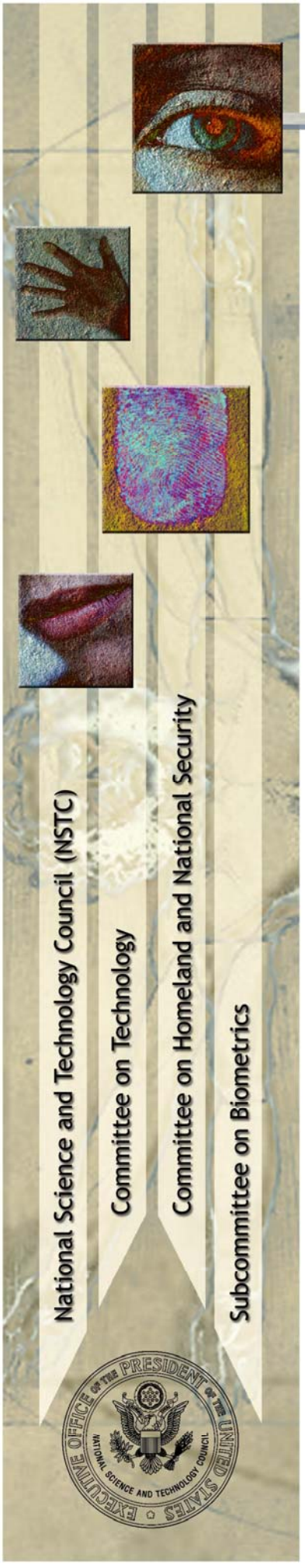


Fingerprint Recognition

Introduction

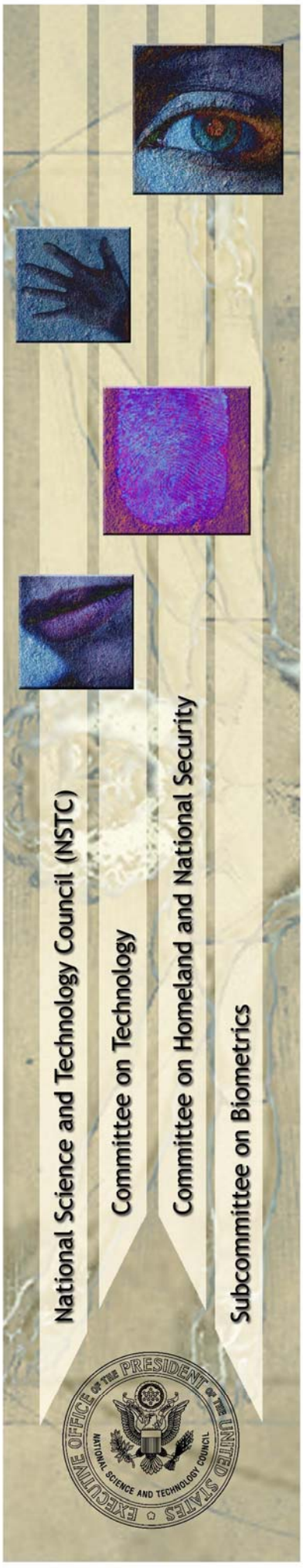
Fingerprint identification is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

History

The practice of using fingerprints as a method of identifying individuals has been in use since the late nineteenth century when Sir Francis Galton defined some of the points or characteristics from which fingerprints can be identified. These "Galton Points" are the foundation for the science of fingerprint identification, which has expanded and transitioned over the past century. Fingerprint identification began its transition to automation in the late 1960s along with the emergence of computing technologies. With the advent of computers, a subset of the Galton Points, referred to as minutiae, has been utilized to develop automated fingerprint technology.

In 1969, there was a major push from the Federal Bureau of Investigation (FBI) to develop a system to automate its fingerprint identification process, which had quickly become overwhelming and required many man-hours for the manual process. The FBI contracted the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), to study the process of automating fingerprint classification, searching, and matching.[1] NIST identified two key challenges: 1 scanning fingerprint cards and extracting minutiae from each fingerprint and 2 searching, comparing, and matching lists of minutiae against large repositories of fingerprints.

In 1975, the FBI funded the development of fingerprint scanners for automated classifiers and minutiae extraction technology, which led to the development of a prototype reader. This early reader used capacitive techniques to collect the fingerprint minutiae (See Hardware section).[2] At that time, only the



individual's biographical data, fingerprint classification data, and minutiae were stored because the cost of storage for the digital images of the fingerprints was prohibitive.[1]

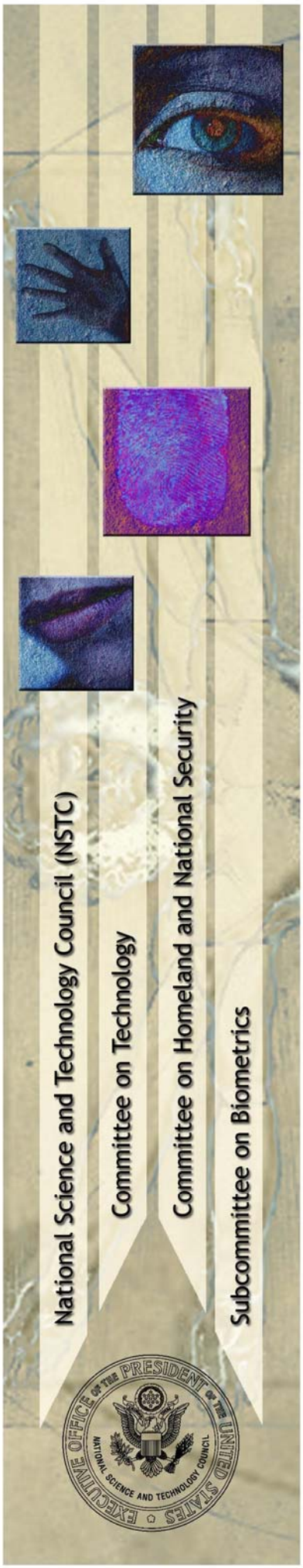
Over the next few decades, NIST focused on and led developments in automatic methods of digitizing inked fingerprints and the effects of image compression on image quality, classification, extraction of minutiae, and matching.[3] The work at NIST led to the development of the M40 algorithm, the first operational matching algorithm used at the FBI[1] for narrowing the human search. The results produced by the M40 algorithm were provided to trained and specialized human technicians who evaluated the significantly smaller set of candidate images. The available fingerprint technology continued to improve and by 1981, five Automated Fingerprint Identification Systems (AFIS) had been deployed.[1] Various state systems within the US and other countries had implemented their own standalone systems, developed by a number of different vendors. During this evolution, communication and information exchange between the systems were overlooked, meaning that a fingerprint collected on one system could not be searched against another system.[1] These oversights led to the need for and development of fingerprint standards.

As the need for an integrated identification system within the US criminal justice community quickly became apparent, the next stage in fingerprint automation occurred at the end of the Integrated Automated Fingerprint Identification System (IAFIS) competition in 1994. The competition identified and investigated three major challenges: 1 digital fingerprint acquisition, 2 local ridge characteristic extraction, and 3 ridge characteristic pattern matching.[4] Demonstrated model systems were evaluated based on specific performance requirements. Lockheed Martin was selected to build the AFIS segment of the FBI's IAFIS project and the major IAFIS components were operational by 1999.[3] Also in this timeframe, commercial fingerprint verification products began to appear for various access control, logon, and benefit verification functions.

Approach

Concept

A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space



and are the low, shallow portion of the friction ridge skin. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path. The images below present examples of fingerprint features: (a) two types of minutiae and (b) examples of other detailed characteristics sometimes used during the automatic classification and minutiae extraction processes.

The types of information that can be collected from a fingerprint's friction ridge impression include the flow of the friction ridges (Level 1 Detail), the presence or absence of features along the individual friction ridge paths and their sequence (Level 2 Detail), and the intricate detail of a single ridge (Level 3 Detail). Recognition is usually based on the first and second levels of detail or just the latter.

AFIS technology exploits some of these fingerprint features. Friction ridges do not always flow continuously throughout a pattern and often result in specific characteristics such as ending ridges, dividing ridges and dots, or other information. An AFIS is designed to interpret the flow of the overall ridges to assign a fingerprint classification and then extract the minutiae detail – a subset of the total amount of information available yet enough information to effectively search a large repository of fingerprints.

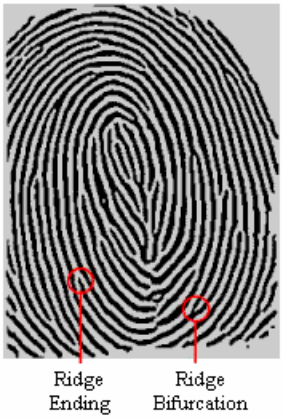


Figure 1: Minutiae.[5]

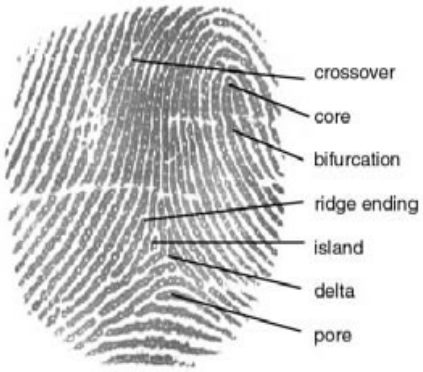
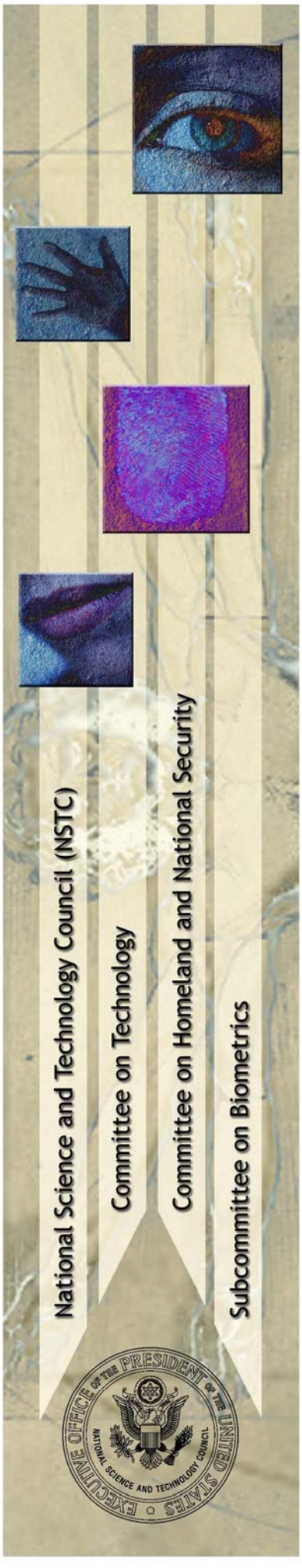


Figure 2: Other Fingerprint Characteristics.[6]

Hardware

A variety of sensor types — optical, capacitive, ultrasound, and thermal — are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today. The



capacitive sensor determines each pixel value based on the capacitance measured, made possible because an area of air (valley) has significantly less capacitance than an area of finger (friction ridge skin). Other fingerprint sensors capture images by employing high frequency ultrasound or optical devices that use prisms to detect the change in light reflectance related to the fingerprint. Thermal scanners require a swipe of a finger across a surface to measure the difference in temperature over time to create a digital image.[7]

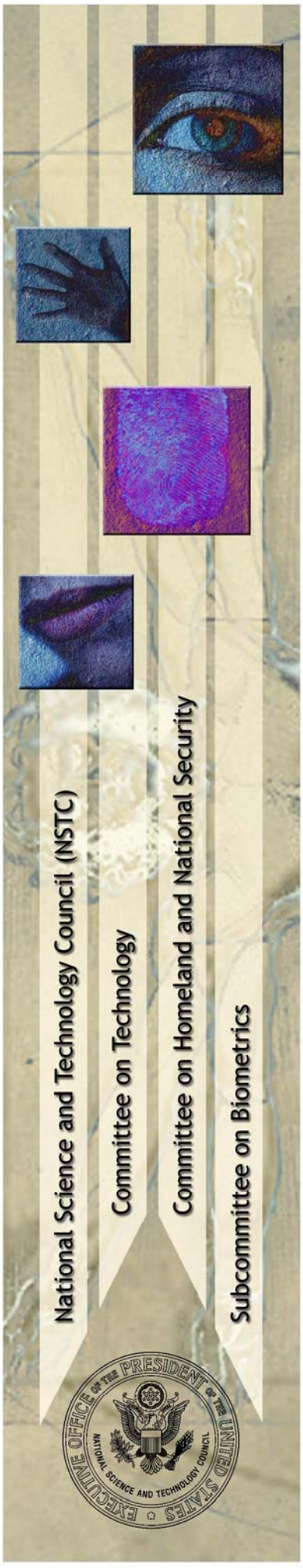
Software

The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. Pattern matching simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching, relies on the minutiae points described above, specifically the location and direction of each point.[4]

United States Government Evaluations

As mandated by the USA PATRIOT ACT and the Enhanced Border Security Act, NIST managed the Fingerprint Vendor Technology Evaluation (FpVTE) to evaluate the accuracy of fingerprint recognition systems.[8] FpVTE was designed to assess the capability of fingerprint systems to meet requirements for both large-scale and small-scale real world applications. FpVTE 2003 consists of multiple tests performed with combinations of fingers (e.g., single fingers, two index fingers, four to ten fingers) and different types and qualities of operational fingerprints (e.g., flat livescan images from visa applicants, multi-finger slap livescan images from present-day booking or background check systems, or rolled and flat inked fingerprints from legacy criminal databases).

The most accurate systems in FpVTE 2003 were found to have consistently very low error rates across a variety of data sets. The variables that had the clearest effect on system accuracy were the number of fingers used and fingerprint quality. An increased number of fingers resulted in higher accuracy: the accuracy of searches using four or more fingers was better than the accuracy of two-finger searches, which was better than the accuracy of single-finger searches.



Standards Overview

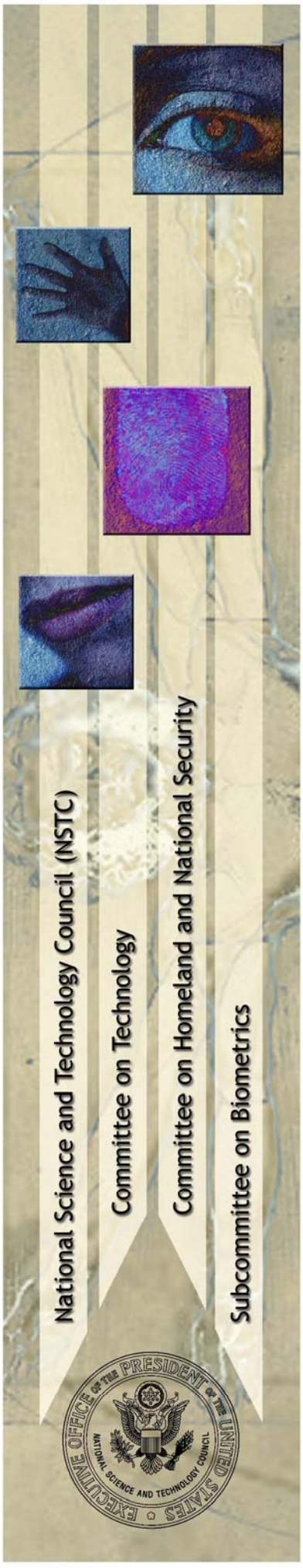
Currently ongoing at both the national and international levels, fingerprints standards development is an essential element in fingerprint recognition because of the vast variety of algorithms and sensors available on the market. Interoperability is a crucial aspect of product implementation, meaning that images obtained by one device must be capable of being interpreted by a computer using another device. Major standards efforts focus on the standardization of the content, meaning, and representation of the fingerprint data interchange formats[9] and include the ANSI/INCITS 381-2004 Finger Image-Based Data Interchange Format, ANSI/INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI-INCITS 378-2004 Finger Minutiae Format for Data Interchange, ISO/IEC 19794-2 Finger Minutiae Format for Data Interchange, ISO/IEC FCD 19794-3 Finger Pattern Based Interchange Format, and the ISO/IEC 19794-4 Finger Image Based Interchange Format.[10] (Additional information regarding these standards can be found in the Appendix.)

Another noteworthy standard is ANSI NIST ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information. This standard specifies a common format used for the exchange of fingerprint, facial, scar, mark and tattoo data effectively across jurisdictional lines or between dissimilar systems made by different manufacturers. Electronic Fingerprint Transmission Specification (v7.1) and Electronic Biometric Transmission Specification (v1.0) are specific implementations of ANSI NIST ITL 1-2000 used by the FBI and DoD. Other standards also associated with ANSI NIST ITL 1-2000 are the FBI's Wavelet Scalar Quantization (WSQ) and Join Photographic Experts Group 2000 (JPEG2000) which are both used for the compression of fingerprint images.

Notable US Government Fingerprint Programs

Fast Capture of Rolled-Equivalent Fingerprints and Palm Prints

Fast capture, a multi-agency Government initiative, is expanding fingerprint and palm research, challenging industry to develop and demonstrate technology to capture 10 rolled-equivalent fingerprints in less than 15 seconds and/or both palm prints in less than one minute, significantly improve fingerprint image quality, reduce the failure-to-enroll rate, and be affordable, rugged,



portable, relatively unobtrusive in size, and deployable in the near future.[11]

Integrated Automatic Fingerprint Identification System (IAFIS)

Maintained by the FBI Criminal Justice Information Services (CJIS), IAFIS contains over 47 million subjects.[12] System capabilities include automated tenprint and latent fingerprint searches, electronic image storage, and electronic exchanges of fingerprints and responses. Through partnerships formed between the FBI and the law enforcement community, IAFIS became operational in 1999 to expedite fingerprint search requests that were being performed manually through human verification — a process that could take up to three months. IAFIS request results are returned within two hours for criminal inquiries and within 24 hours for civil inquiries.[12]

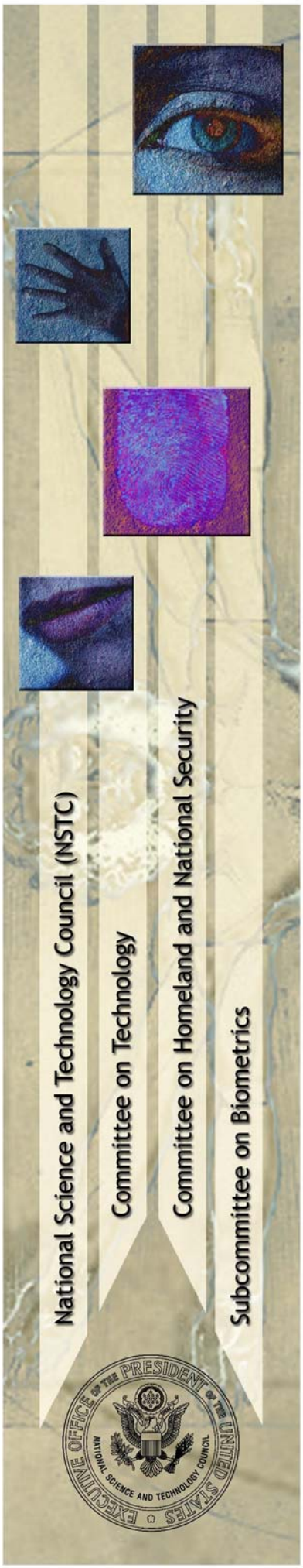
NIST Special Publication 800-76

NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, contains specifics for acquiring, formatting, and storing fingerprint images and templates for collecting and formatting facial images; and specifications for biometric devices used to collect and read fingerprint images. The publication specifies that two fingerprint be stored on the card as “minutia templates,” mathematical representations of fingerprint images.[13]

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 to and departure from the US.

Most visitors experience US-VISIT's biometric procedures — digital, inkless fingerprints and digital photographs — upon entry to the US. In those cases where a visitor requires a visa, the Department of State collects the visitor's biometric and biographic information. When the visitor arrives in the US, US-VISIT procedures allow the Department of Homeland Security to determine whether the person applying for entry is the same person who was issued the visa by the Department of State.



Summary

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. The determination and commitment of the fingerprint industry, government evaluations and needs, and organized standards bodies have led to the next generation of fingerprint recognition, which promises faster and higher quality acquisition devices to produce higher accuracy and more reliability. Because fingerprints have a generally broad acceptance with the general public, law enforcement, and the forensic science community, they will continue to be used with many governments' legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric.

Document References

[1] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

[2] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

[3] James Wayman, et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).

[4] Maltoni, Davide, Maio, Jain, and Prabhakar, Handbook of Fingerprint Recognition (Springer: New York, 2005).

[5] Secugen Biometrics Solutions <http://www.secugen.com/images/faq02.gif>.

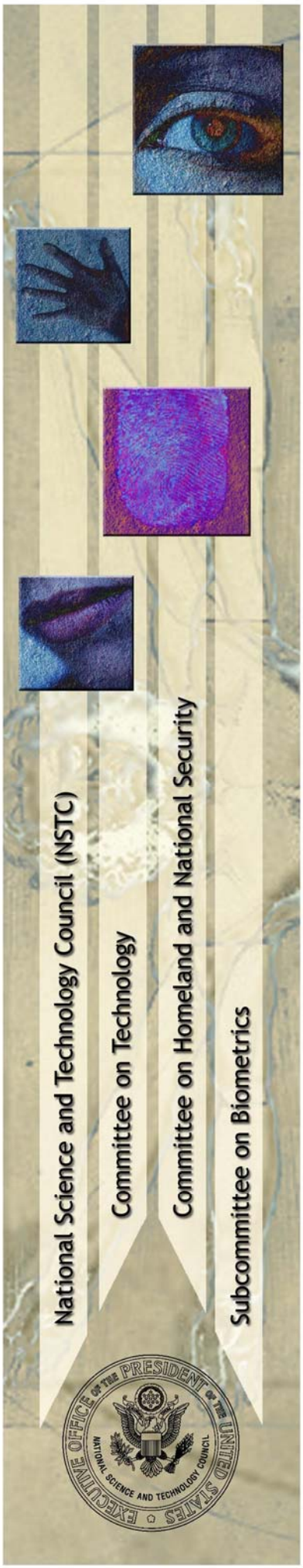
[6] International Biometric Group <http://www.biometricgroup.com>.

[7] Manfred Bromba, "Bioidentification: Frequently Asked Questions" <http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren>.

[8] FpVTE 2003: "Fingerprint Vendor Technology Evaluation" 6 July 2004 < http://fpvte.nist.gov/>.

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

[10] International Organization for Standardization, "JTC 1/ SC37 Biometrics Projects"



<http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=5537&scopelist=PROGRAMME>.

[11] NSTC Subcommittee on Biometrics, "Fingerprint Recognition Interagency Coordination Plan" January 2006.

[12] FBI IAFIS "Integrated Automated Fingerprint Identification System: What is it?" 30 June 2005 <http://www.fbi.gov/hq/cjisd/iafis.htm>.

[13] National Institute of Standards and Technology, Computer Security Division: Computer Security Resource Center, "Personal Identity Verification (PIV) of Federal Employees/Contractors" 24 March 2006 <http://csrc.nist.gov/piv-program/index.html>.

Appendix

ANSI/INCITS 381-2004 Finger Image Based Data Interchange Format — This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.

For more information, see the following: http://www.incits.org.

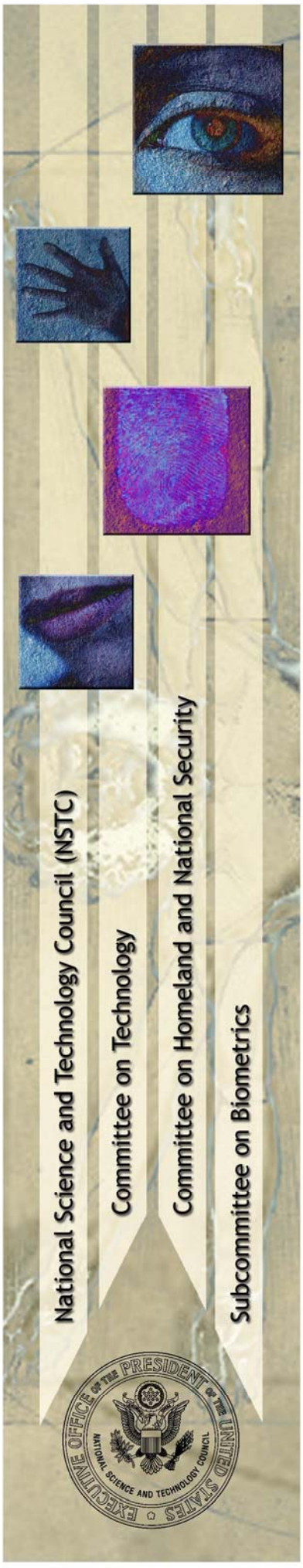
ANSI/INCITS 377-2004 Finger Pattern Based Interchange Format — This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.

For more information, see the following: http://www.incits.org.

ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange -- This standard defines a method of representing fingerprint information using the concept of minutiae. It defines the placement of the minutiae on a fingerprint, a record format for containing the minutiae data, and optional extensions for ridge count and core/delta information.

For more information, see the following: http://www.incits.org.

ANSI/NIST ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information — This



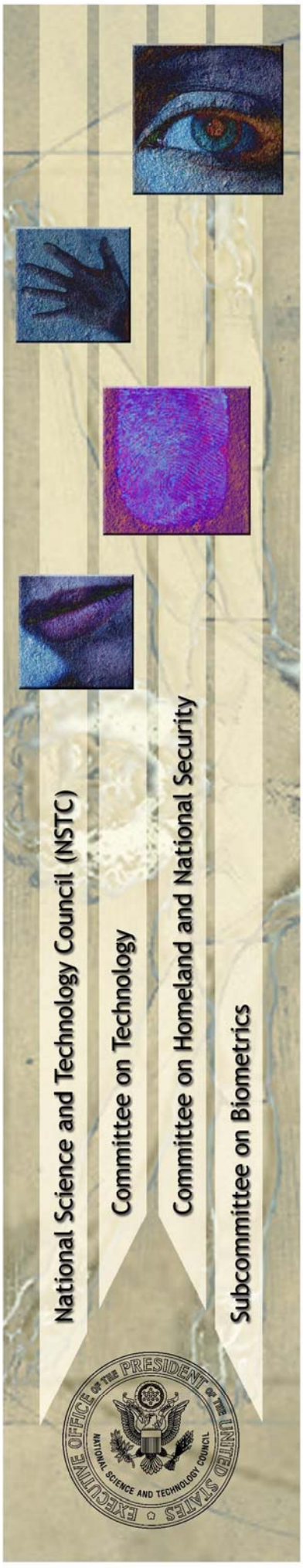
standard defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mugshot, and scar, mark, & tattoo (SMT) image information that may be used in the identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images.

For more information, see the following: ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf

ISO/IEC 19794-2 Finger Minutiae Format for Data Interchange — This standard describes how minutiae points shall be determined, defines data formats for containing the data for general and smart card use, and details conformance information. Guidelines and values for matching and decision parameters are provided as an informative Annex. The standard defines three types of minutiae, including ridge ending and ridge bifurcation. The adopted minutiae determination strategy relies on skeletons derived from a digital fingerprint image. For more information, see the following: http://www.iso.org.

ISO/IEC FCD 19794-3 Finger Pattern Based Interchange Format — This draft standard specifies that a fingerprint image is divided into a grid of overlapping or non-overlapping cells. At each cell, the finger pattern will be represented by a cell structure. A method to obtain the cell structure is to decompose each of the cells into a two-dimensional spectral representation such as the two-dimensional Discrete Fourier Transform (DFT). The decomposition produces spectral components, where each component can be characterized by a wavelength in the horizontal (x) and vertical (y) directions, amplitude, and a phase. For more information, see the following: http://www.iso.org.

ISO/IEC 19794- 4 Finger Image Based Interchange Format — This standard specifies that the image shall appear to have been captured in an upright position and shall be approximately centered horizontally in the field of view. The scanning sequence and recorded data shall appear to have been from left-to-right, progressing from top-to bottom of the fingerprint. The origin of the axes, pixel location (0,0), is at the upper left hand corner of each image with the x-coordinate (horizontal) position increasing positively from the origin to the right side of the image while the y-coordinate (vertical) position increasing positively from the origin to the bottom of the image. It also specifies that the



header must be CBEFF compliant. For more information, see the following: http://www.iso.org.

ISO/IEC 19794-8 Finger Pattern Skeletal Data — This standard it is intended to be used to achieve interoperability between pattern and minutiae-based fingerprint recognition systems. It is based on the common properties shared between the spectral pattern and minutia by encoding ridges in a manner that the skeleton of the ridge provides the basis for detecting a minutia.

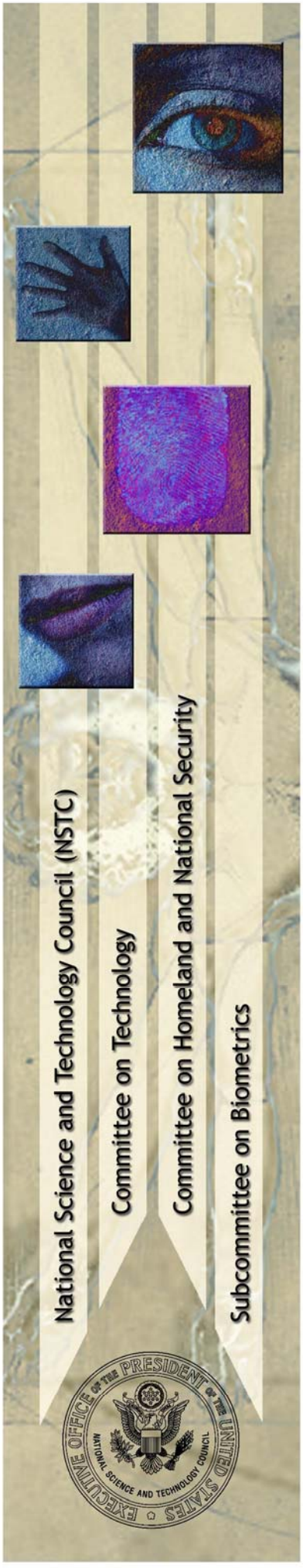
For more information, see the following: http://www.iso.org.

EFTS v7.1 Electronic Fingerprint Transmission Specification — This specification covers electronic transmission of information involving fingerprints to the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) based on the ANSI NIST ITL 1-2000 strandard. The purpose of this document is to specify certain requirements to which agencies must adhere to communicate electronically with the IAFIS. For more information, see http://www.fbi.gov/filelink.html?file=/hq/cjisd/iafis/efts71/efts71.pdf.

EBTS v1.0 Electronic Biometric Transmission Specification — This specification describes customizations of the Federal Bureau of Investigation (FBI) Electronic Fingerprint Transmission Specification (EFTS) transactions that are necessary to utilize the Department of Defense (DoD) Automated Biometric Identification System (ABIS).

FBI- WSQ (Wavelet Scalar Quantization) Fingerprint Image Compression — WSQ is a lossy compression that is able to preserve the high resolution details of gray scale images that are usually discarded by other lossy compression algorithms. It achieves high compression ratio, on average 15:1 depending on parameters. For more information, see the ”Criminal Justice Information Services (CJIS) WSQ Gray-scale Fingerprint Image Compression Specification,” Federal Bureau of Investigation, Document No. IAFIS-IC-0110 (V3), 19 December 1997.

JPEG2000 (Joint Photographic Experts Group 2000) — Fingerprint Image Compression is a new image coding system that uses state-of-the-art compression techniques based on wavelet technology. Its architecture should lend itself to a wide range of uses from portable digital cameras through to advanced pre-press, medical imaging and other key sectors.



About the National Science and Technology Council

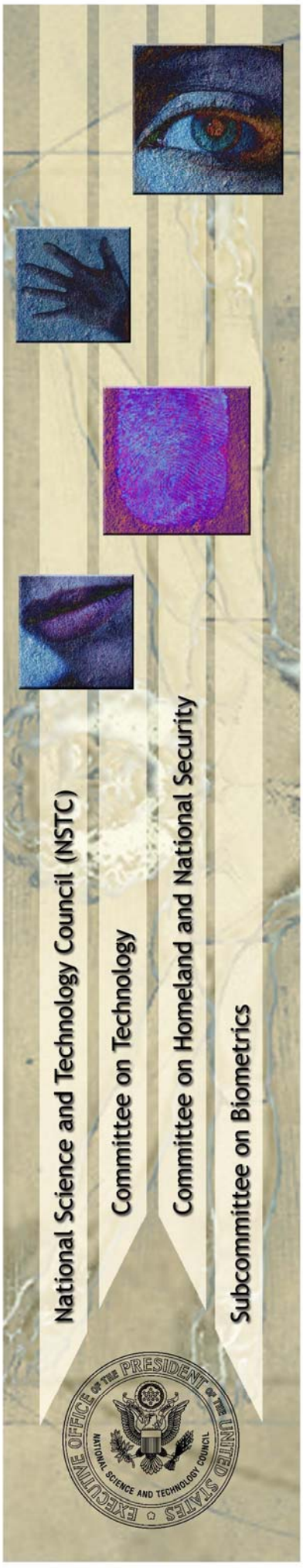
The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development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

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)

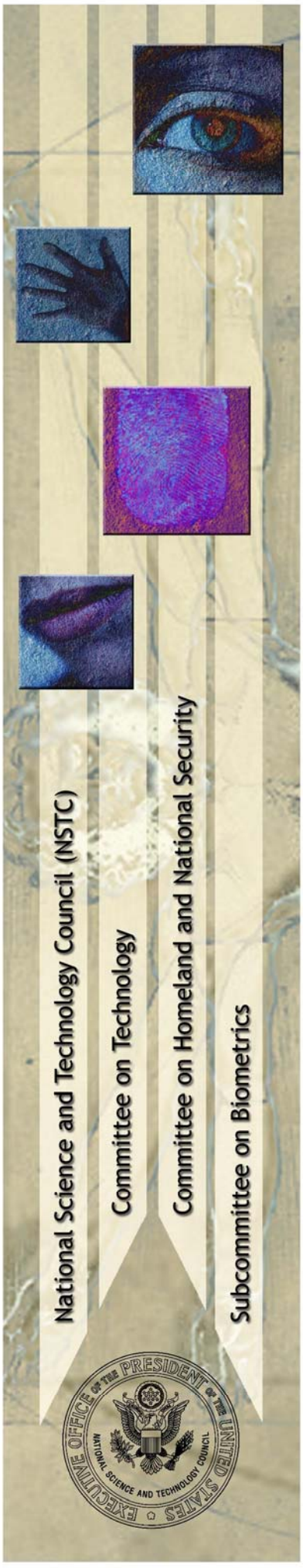
Ms. Valerie Lively (DHS S&T)

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. Jim Zok (DOT)

Mr. David Young (FAA)

Special Acknowledgements

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

- Kelly Smith, BRTRC, for performing background research and writing the first draft
- The Standards ICP Team, B. Scott Swann and others from the FBI's CJIS Division, and Stephen Meagher and associates in the FBI Laboratory Division for reviewing the document and providing numerous helpful comments
- The Fingerprint Recognition ICP Team for their exhaustive work compiling historical and current information and for highlighting those that should be included in this document

Document Source

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