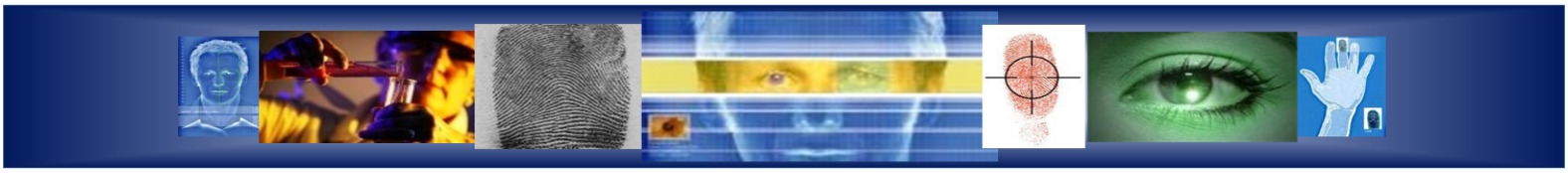


Version 1.0

Biometrics Glossary (BG)

Feb 1, 2008

A

American National Standards Institute (ANSI)

A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The mission of ANSI is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Analyze

Converts data to actionable information and recommendations as applicable to increase situational awareness and better understand possible courses of action.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Arch

A fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Associated Information

Non-biometric information about a person. For example, a person's name, personal habits, age, current and past addresses, current and past employers, telephone number, email address, place of birth, family names, nationality, education level, group affiliations, and history, including such characteristics as nationality, educational achievements, employer, security clearances, financial and credit history.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Attempt

The submission of a single set of biometric samples to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual.

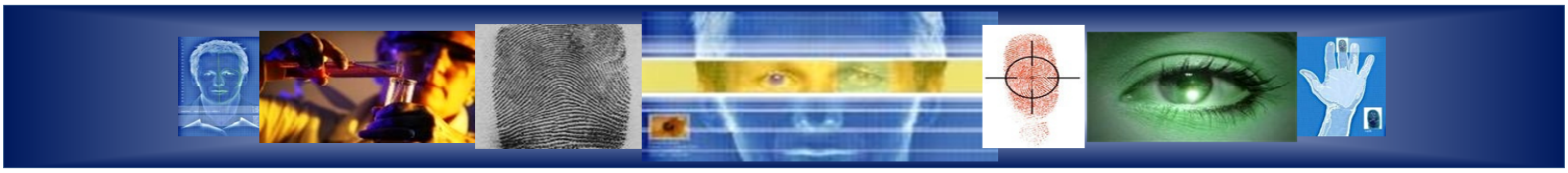
National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Authoritative Source

The primary DoD-approved repository of biometric information on a biometric subject. The authoritative source provides a strategic capability for access to standardized, comprehensive, and current biometric files within the DoD and for the sharing of biometric files with Joint, Interagency, and designated Multinational partners. The DoD may designate authoritative sources for various populations consistent with applicable law, policy and directives.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006



Biometrics Glossary (BG)

Auto-correlation

A proprietary finger scanning technique. Two identical finger images are overlaid in the auto-correlation process, so that light and dark areas, known as Moiré fringes, are created.

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

http://www.afb.org.uk/docs/glossary.htm

Automated Biometric Identification System (ABIS)

Department of Defense (DoD) system implemented to improve the U.S. government's ability to track and identify national security threats.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Automated Fingerprint Identification System (AFIS)

A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc).

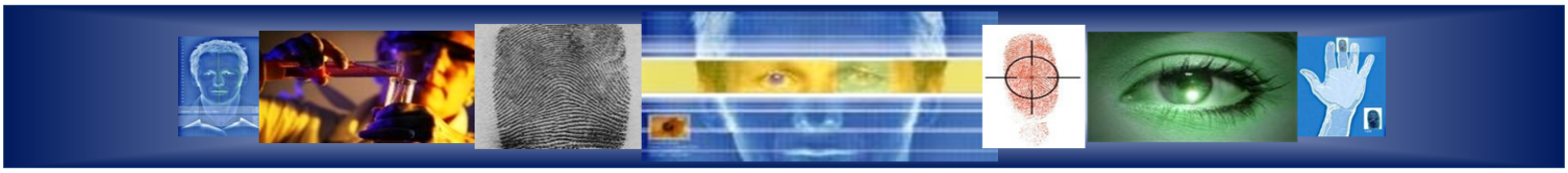
National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Automated Identification Management System (AIMS)

A system that acts as a central web-based informational portal between U.S. Central Command (USCENTCOM), National Ground Intelligence Center (NGIC), and the Biometrics Fusion Center (BFC) that is designed to fuse intelligence analysis and value added comments from field users of matched biometric and biographic data.

USCENTCOM Biometric Identification System for Access (BISA) CONOPS



Biometrics Glossary (BG)

B

Behavioral Biometric Characteristic

A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biographic Data

Data that describes physical and non-physical attributes of a biometric subject from whom biometric sample data has been collected. For example, full name, age, height, weight, address, employers, telephone number, email address, birthplace, nationality, education level, group affiliations, also data such as employer, security clearances financial and credit history.

Derived from USCENTCOM Biometric Identification System for Access (BISA) CONOPS

Biological Biometric Characteristic

A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristics. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biometrically Enabled Intelligence

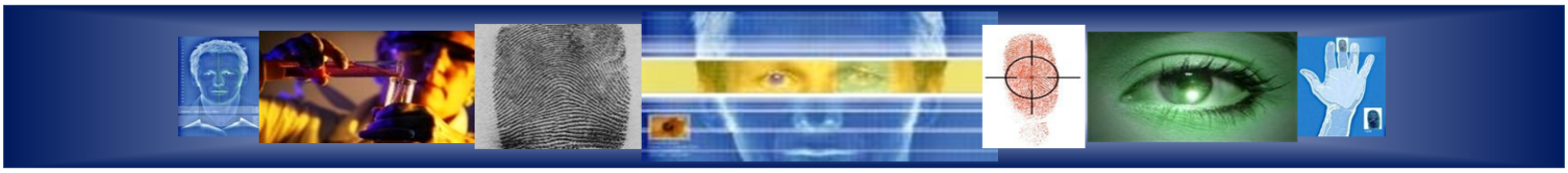
Intelligence information associated with biometrics data e.g. pattern analysis of a biometric subject's encounters with biometrics systems, judgments about a biometric subject disposition or intent based on biometric matches with forensic data, etc.

Derived from DoD D 852I.AAE DoD BIOMETRICS PROGRAM

Biometrically Enabled Physical Access

The process of granting access to installations and facilities through the use of biometrics.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006



Biometrically Enabled Watchlist (BEWL)

Any list of person of interests (POI), with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions for each individual. However, there first must be an acceptable degree of certainty that there is some indication of past behavior attributable to the individual that belongs to the biometric sample in order to estimate the level of threat posed by that individual. Even upon encounter or capture, we may never know an individuals' true identity, but that is immaterial as long as the linkage between the biometric sample and past threat behavior is established. No practicable standard currently exists for BEWLs, but the minimum content of a BEWL record is (1) a biometric identity (biometric sample linked to a POI), (2) a category of interest or threat commonly referred to as a tier, (3) the recommended action(s) to taken upon next encounter, and (4) notification instructions. The classification of the information within the BEWL can be up to TS/SCI/ORCON. In most instances the information will be releasable or at the UNCLASSIFIED//FOUO level to facilitate sharing.

The DoD Biometrically-Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

Biometric Application Decision

A conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Automated Toolset (BAT)

A multimodal biometric system that collects and compares fingerprints, iris images and facial photos. It is used to enroll, identify and track persons of interest; build digital dossiers on the individuals that include interrogation reports, biographic information, relationships, etc. BAT has an internal biometric signature searching and matching capability.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Biometric Capture Device

A device that collects a signal from a biometric characteristic and converts it to a captured biometric sample.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

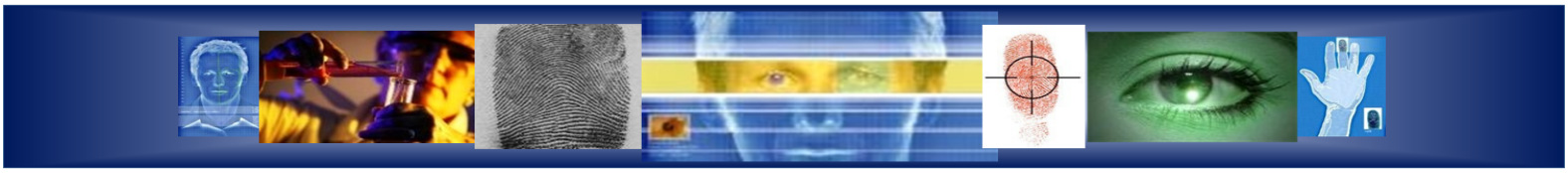
Biometric Capture Process

A process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Characteristic

A biological and behavioral characteristic of a biometric subject that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of biometric subjects.



Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Claim

A claim that a biometric subject is or is not the source of a specified or unspecified biometric reference.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Database

A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related biometric subject information, etc.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Biometric Data Block

A block of data with a defined format that contains one or more biometric samples or biometric templates.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Feature

Numbers or labels extracted from biometric samples and used for comparison.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Feature Extraction Process

A process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from the other biometric samples.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric File

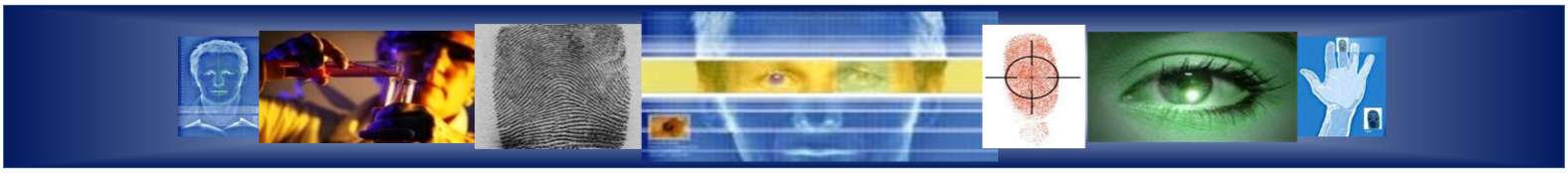
The standardized individual data set resulting from a collection action (biometric sample and contextual data).

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Biometric Identification Application

A system which contains an open-set or closed-set identification application.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007



Biometric Identification System for Access (BISA)

A biometric and contextual data collection and credential card production system. It is capable of multi-modal biometric collection (fingerprint, iris, and facial recognition). The system collects biometric and biographical information from visitors to U.S., Coalition, and allied installations worldwide. It produces biometric enabled identification cards compatible with the Common Access Card (CAC) readers. The identification cards (which are counterfeit deterrent, tamper proof and encrypted), use fingerprint images to conduct one-to-one identity verification. BISA collects, transmits, stores, retrieves, manipulates, and displays biometric and contextual data in accordance with national/international standards and industry best practices.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

Biometric Intelligence Resource (BIR)

A system that has been established to provide members of the DoDIIS Intelligence Community and theater war fighters with access to a reliable, centralized, and permanent repository of potential terrorist biometric information and associated intelligence information. The BIR system ingests biometric signatures and contextual data collected from Department of Defense biometric processing systems and makes this information available to members of the worldwide Intelligence Community through a web-based interface for the purpose of positive identification of individuals and tracking related intelligence.

Derived from Biometric Intelligence Resource (BIR) Implementation: 2006-2007 BIR Version 2 System Design Document (SDD) 20 June 2007

Biometric Property

The descriptive attributes of the biometric subject estimated or derived from the biometric sample by automated means.
EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch whorl and loop types. In the case of facial recognition, this could be estimates of age or gender.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Biometric Reference

One or more stored biometric samples, biometric templates or biometric models attributed to a biometric subject and used for comparison.
EXAMPLE Face image on a passport; fingerprint minutia(e) template on a National ID card; Gaussian Mixture Model for speaker recognition, in a database.

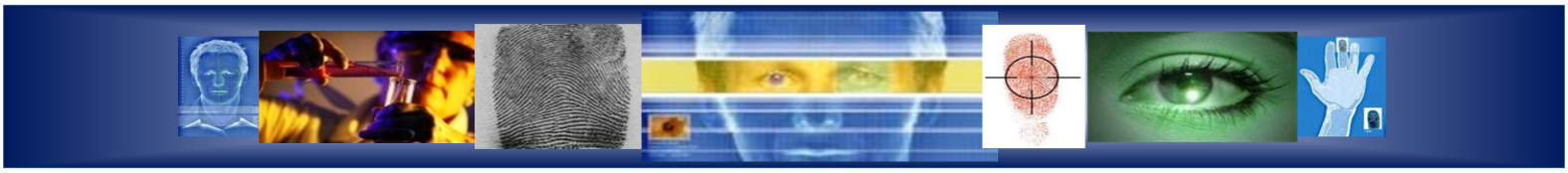
JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

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 a biometric subject based on measurable biological (anatomical and physiological) and behavioral characteristics.

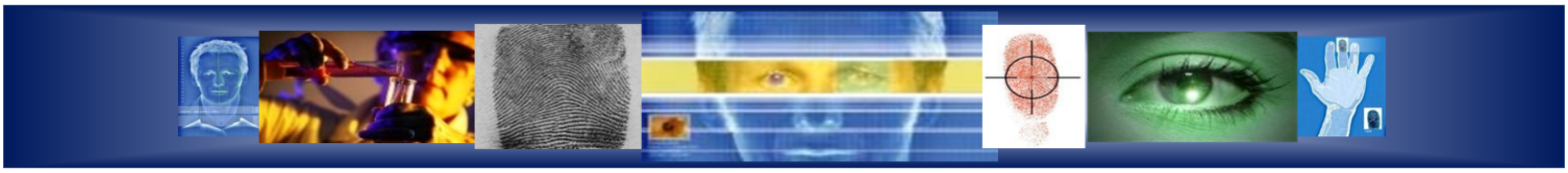
National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



Biometrics Glossary (BG)

Biometric Sample	One of two components of a biometric file (biometric samples and contextual data). Data that represents a biometric characteristic of a biometric subject as captured by a biometric system. *Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006*
Biometric Sample Collector	An individual trained in biometrics that is familiar with employment of biometrics in support of his or her organization, performing the biometric sample(s) collection. *Biometrics Task Force & Biometrics Data Team*
Biometrics Application Programming Interface (BioAPI)	Defines the application programming interface and service provider interface for a standard biometric technology interface. The BioAPI enables biometric devices to be easily installed, integrated or swapped within the overall system architecture. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Biometrics Enterprise	All systems, interfaces and personnel that are utilized to establish identities of people through the use of biometric modalities. *Biometrics Task Force Strategy Division*
Biometrics Program	A comprehensive process incorporating the principles and practices of biometrics into an organization. *DoD D 852I.AAE DoD BIOMETRICS PROGRAM*
Biometric Subject	An individual for which biometric samples were collected and enrolled into a biometric database for the purpose of identification and/or verification. *Biometrics Task Force & Biometrics Data Team*
Biometric System	Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of: 1. Capturing a biometric sample from a biometric subject. 2. Extracting and processing the biometric data from that sample. 3. Storing the extracted information in a database. 4. Comparing the biometric data with data contained in one or more references. 5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved. A biometric system may be a component of a larger system. *Derived from National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*



Biometric Template

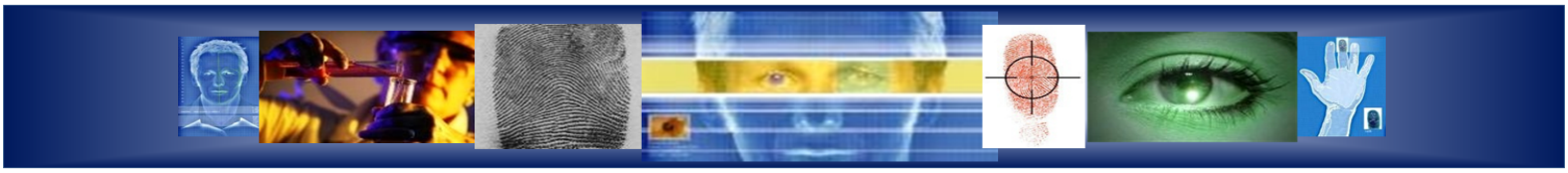
Set of stored biometric features comparable directly to biometric features of a recognition biometric sample.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Blue Force

A population group of trusted individuals including, but not limited to, DoD personnel and family members, U.S. persons, trusted allies, and coalition members.

DoD D 852I.AAE DoD BIOMETRICS PROGRAM



C

Challenge Response

A method used to confirm the presence of an individual by eliciting direct responses from the individual. Responses can be either voluntary or involuntary. In a voluntary response, the individual will consciously react to something that the system presents. In an involuntary response, the individual body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Closed-set Identification

A biometric task where an unidentified biometric subject is known to be in the database and the system attempts to determine his/her identity. Performance is measured by the frequency with which the biometric subject appears in the system's top rank (or top 5, 10, etc.).

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Collect

Capture biometric and related contextual data from a biometric subject, with or without his knowledge. Create and transmit a standardized, high-quality biometric file consisting of a biometric sample and contextual data to a data source for matching.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Common Access Card (CAC)

The standards identification card for active duty personnel (to include the selected reserve), DoD civilian personnel, and eligible contractor personnel. It is the principal card used to enable physical access to buildings and controlled spaces and can be used to gain access to the department's computer networks and systems. The card, which accommodates an integrated circuit chip, also contains other relevant media such as magnetic strips and bar codes.

DoD Deputy Secretary of Defense Memorandum, Smart Card Adoption and Implementation, 10 November 1999

Common Biometric Exchange File Format (CBEFF)

A standard that provides the ability for a system to identify, and interface with multiple biometric systems, and to exchange data between system components.

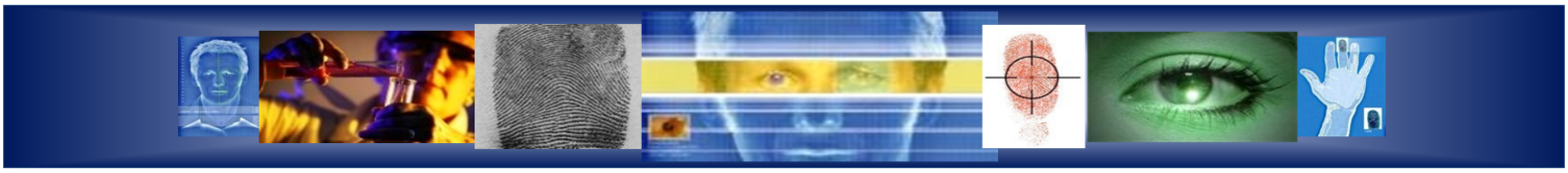
National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Common Biometric Exchange Formats Framework (CBEFF) specification

Describes a set of data elements necessary to support biometric technologies in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

National Institute of Standards and Technology Interagency Report (NISTIR) 6529-2001, Common Biometric Exchange File Format, 3 January 2001



Comparison

Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Comparison Decision

Determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies), including a threshold, and possibly other inputs.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Contextual Data

Elements of biographical and situational information (who, what, when, where, how, why, etc.) that are associated with a collection event and permanently recorded as an integral component of the biometric file.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Core Point

The 'center(s)' of a fingerprint. In a whorl pattern, the core point is found in the middle of the spiral/circles. In a loop pattern, the core point is found in the top region of the innermost loop. More technically, a core point is defined as the topmost point on the innermost upwardly curving friction ridgeline. A fingerprint may have multiple cores or no cores.

National Science & Technology Council (NSTC), 14 September 06

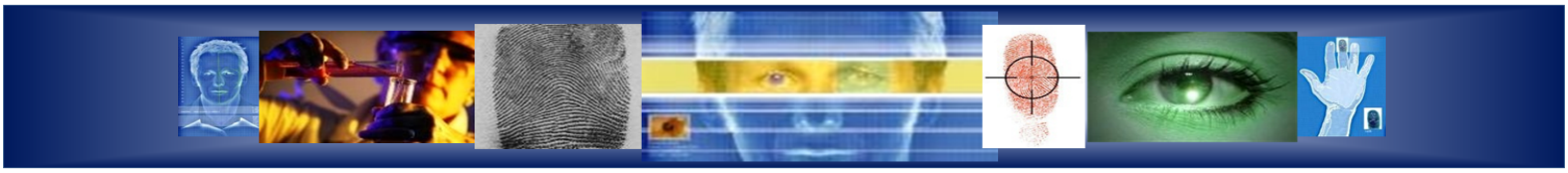
http://www.biometrics.gov/Documents/glossary.pdf

Cumulative Match Characteristic (CMC)

A method of showing measured accuracy performance of a biometric system operating in the closed-set identification task. Templates are compared and ranked based on their similarity. The CMC shows how often the biometric subject template appears in the ranks (1, 5, 10, 100, etc.), based on the match rate. A CMC compares the rank (1, 5, 10, 100, etc.) versus identification rate.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



D

Decide/Act

The response by the operational or business process owner (either automated or human-in-the-loop) to the results of the match and/or analysis described in the DoD Biometric Process, as well as associated information relevant to the situation.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Defense Biometrics Identification System (DBIDS)

A DoD owned and operated system developed by Defense Manpower Data Center (DMDC) as a force protection program to manage installation access control for military installations. It is a networked client/server database system designed to easily verify the access authorization of personnel and fingerprint biometric identification. The DBIDS software application is used to enter personnel and vehicle data into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time.

Defense Biometric Identification System User Manual, May 24, 2006

Degrees of Freedom

A statistical measure of how unique biometric data is. Technically, it is the number of statistically independent features (parameters) contained in biometric data.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Delta Point

The part of a fingerprint pattern that looks similar to the Greek letter delta. Technically, it is the point on a friction ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Detainee Reporting System (DRS)

A System designed to support the processing of prisoner of wars (POWs) and detainees by issuing Identification Serial Numbers (ISNs), collecting identifying information, recording medical histories, maintaining property records, issuing transfer, release, death, and other orders providing dispositions to detainees, maintain a tribunal history, and track changes to detainee records and other general information relevant to the detainee.

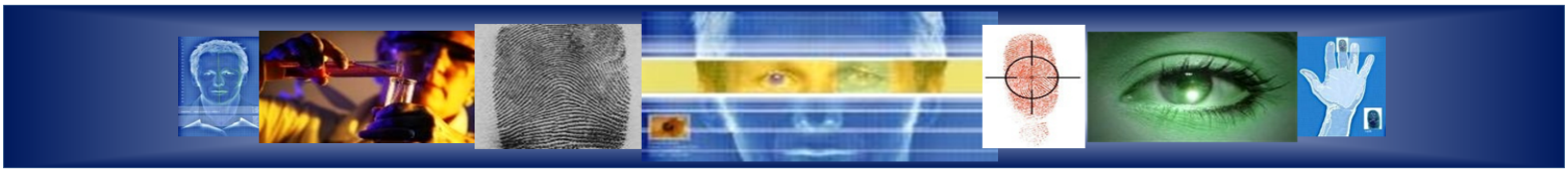
Derived from Detainee Reporting System courtesy of National Detainee Reporting Center, August 06

Detection and Identification Rate

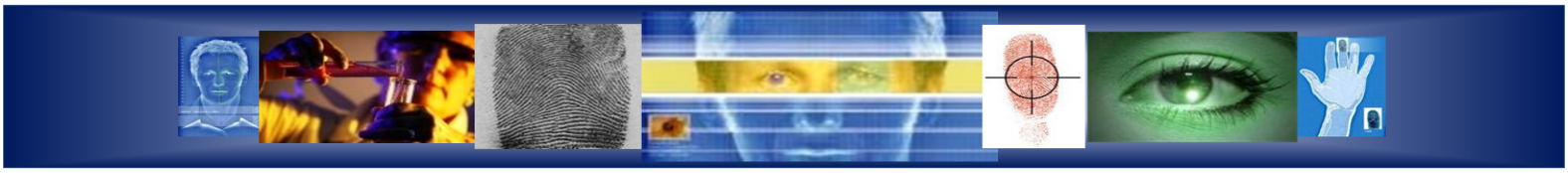
The rate at which biometric subjects, who are in a database, are properly identified in an open-set identification (watchlist) application.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



Detection Error Trade-off (DET) Curve	A graphical plot of measured error rates. DET curves typically plot matching error rates (false non-match rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate). *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Difference Score	A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference. *National Science & Technology Council (NSTC), 14 September 06* *http://www.biometrics.gov/Documents/glossary.pdf*
Duplicate Enrollment Check	The comparison of a recognition biometric sample/biometric feature/biometric model to some or all of the biometric references in the enrollment database to determine if any similar biometric reference exists. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*



E

Electronic Biometric Transmission Specification (EBTS)

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). Any DoD entity that wishes to interface with the DoD ABIS must conform to the DoD EBTS.

Department of Defense
Electronic Biometric Transmission Specification
23 August 2005 Version 1.1 DIN: DOD_BMO_TS_EBTS_Aug05_01.01

Electronic Fingerprint Transmission Specification (EFTS)

A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS). This specification facilitates information sharing and eliminates the delays associated with fingerprint cards.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Enroll

Create and store, for a biometric subject, an enrollment data record that includes biometric reference(s) and typically, non-biometric data.

Derived from JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Enrollment

The process of collecting a biometric sample from a biometric subject, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

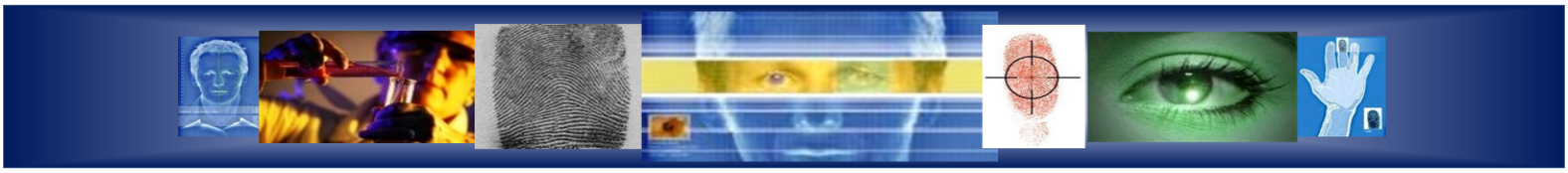
Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Expanded Maritime Interdiction Operation (EMIO)

A key maritime component needed to support the global war on terrorism by deterring, delaying, and disrupting the movement of terrorists and terrorist-related materials and personnel at sea. U.S. Navy ships operating in the Central Command's (CENTCOM) Area of Responsibility (AOR) have the capability to collect and forward biometric data from potential terrorists for searching against databases.

Derived from Biometrics Task Force And Navy Team for Success January 2007



F

Face Recognition

A biometric modality that uses an image of the visible physical structure of a biometric subject's face for recognition purposes.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Acquire (FTA)

Failure of a biometric system to capture and/or extract usable information from a biometric sample.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Acquire Rate

The frequency of a failure to acquire.

National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

Failure to Enroll (FTE)

Failure of a biometric system to form a proper enrollment reference for a biometric subject. Common failures include biometric subjects who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Failure to Enroll Rate

The probability that a biometric system will have a failure-to-enroll.

National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

False Acceptance

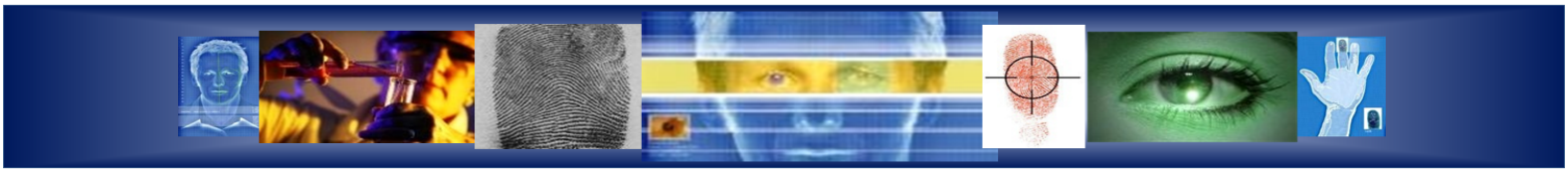
When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates an imposter against a claimed identity.

Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

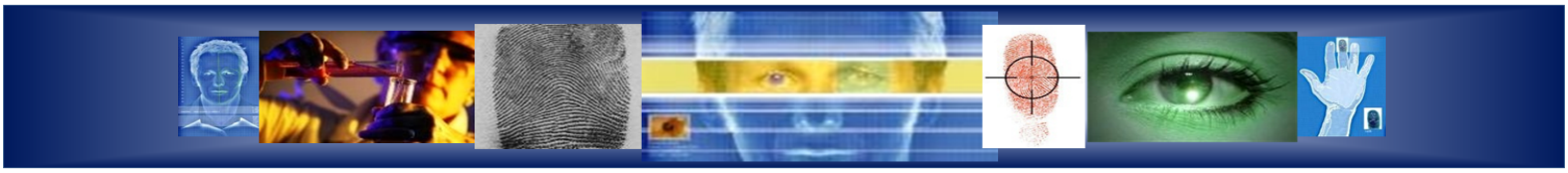
False Acceptance Rate (FAR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false acceptance, which occurs when a biometric subject is incorrectly matched to another biometric subject's existing biometric. Example: Frank claims to be John and the system verifies the claim.

Derived from National Science & Technology Council (NSTC), 14 September 06



	http://www.biometrics.gov/Documents/glossary.pdf
False Alarm Rate	A statistic used to measure biometric performance when operating in the open-set identification (sometimes referred to as watchlist) task. This is the percentage of times an alarm is incorrectly sounded on a biometric subject who is not in the biometric system's database (the system alarms on Frank when Frank isn't in the database), or an alarm is sounded but the wrong biometric subject is identified (the system alarms on John when John is in the database, but the system thinks John is Steve). *Derived from National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Match	The comparison decision of 'match' for a recognition biometric sample and a biometric reference that are not from the same source. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
False Match Rate (FMR)	A statistic used to measure biometric performance. Similar to the False Acceptance Rate (FAR). *Derived from National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Non-Match	A comparison decision of 'no-match' for a recognition biometric sample and a biometric reference that are from the same source. *JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007*
False Non-Match Rate (FNMR)	A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not. *National Science & Technology Council (NSTC), 14 September 06* http://www.biometrics.gov/Documents/glossary.pdf
False Rejection	The failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject. *Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)*
False Rejection Rate (FRR)	A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false rejection. A false rejection occurs when a biometric subject is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim.



Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Features

Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Fingerprint

The image left by the minute ridges and valleys found on the hand of every person. In the fingers and thumbs, these ridges form patterns of loops, whorls and arches.

Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints
http://www.fbi.gov/hq/cjisd/takingfps.html

Fingerprint Recognition

A biometric modality that uses the physical structure of an biometric subject's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutia(e) points that include bifurcations and ridge endings.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Fingerprint Scanning

Acquisition and recognition of a biometric subject's fingerprint characteristics for identification purposes. This process allows the recognition of a biometric subject through quantifiable physiological characteristics that detail the unique identity of an individual.

Derived from The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines . Version 1.03, September 2003
http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf

Fingerprint Vendor Technology Evaluation (2003) (FpVTE)

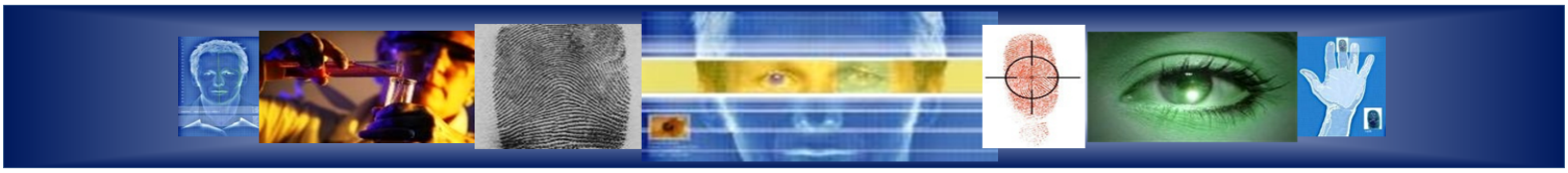
An independently administered technology evaluation of commercial fingerprint matching algorithms.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Force Protection (FP)

Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information by using biometrics to positively link identity information to a given physical individual. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP.

Derived from Joint Publication 3-0, Joint Operations,17 September 2006
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf



Foreign Humanitarian Assistance (FHA)

Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Foreign humanitarian assistance (FHA) provided by US forces is limited in scope and duration. The foreign assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing FHA. FHA operations are those conducted outside the United States, its territories, and possessions. Also called FHA. Biometrics can be used as an enabler for personal identification for humanitarian assistance distribution.

Derived from Joint Publication 3-0, Joint Operations,17 September 2006

http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf

Forensic

Relates to the use of science or technology in the investigation and establishment of facts or evidence. Collected biometric samples could then be linked to non-biometric forensic evidence.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Friction Ridge

The ridges present on the skin of the fingers and toes, and on the palms and soles of the feet, which make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Friendly

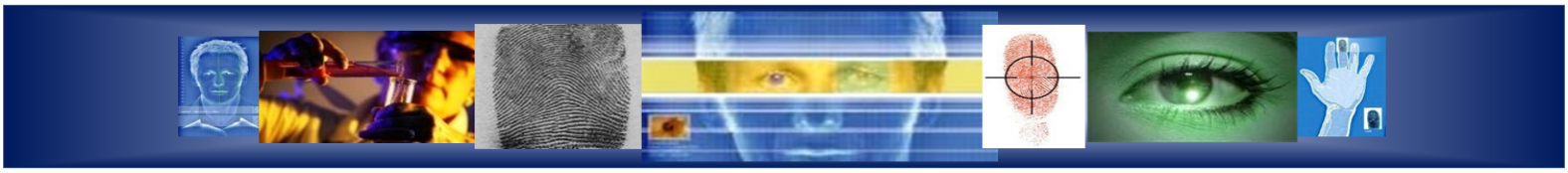
Trusted individuals, DoD personnel and family members, US Persons, trusted Allies, Coalition, etc.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Full Enrollment

Enrollment of biometric data on a subject that includes 14 fingerprint images (4 slaps, 10 rolls), 5 face photos, 2 irises, and required text fields. The sample must be EBTS compliant. Typically used for detainees, locally hire screenings, and other applications.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07



G

Gait

A biometric subject's manner of walking. This behavioral characteristic is in the research and development stage of automation.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Gallery

The biometric system's database, or set of known biometric subjects, for a specific implementation or evaluation experiment.

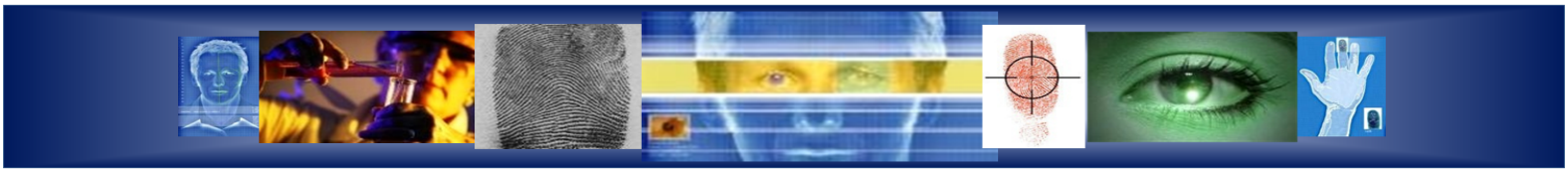
Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Gray Force

A general term used to describe civilian personnel. However, the term may also be applied to defined individuals for whom no identity has been positively established. It may include those individuals that have not been positively identified as being either hostile (Red) or friendly (Blue). In general use, it has become a term similar to "Boggy", which is used by aviation personnel to indicate that they have acquired contact (visual or radar) with another aircraft but have not identified it as being friendly or hostile ("Bandit"). A population group of unknown individuals including, but not limited to, nonaligned persons, host country and third-country nationals, and non-U.S. citizens.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07



H

Hamming Distance (HD)

The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Hand Geometry Recognition

A biometric modality that uses the physical structure of a biometric subject's hand for recognition purposes.

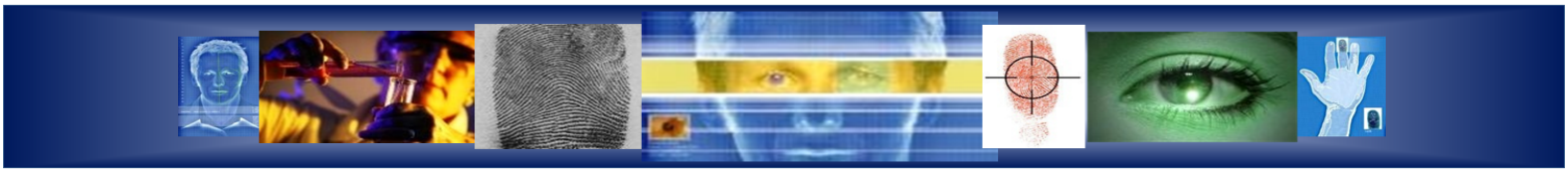
Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Hand Scan

Print from the outer side of the palm.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07



Biometrics Glossary (BG)

I

Identification

The one-to-many (1:N) process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the biometric subject whose template was matched.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identification Rate

The rate at which a biometric subject in a database is correctly identified.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Identifier

A unique data string used as a key in the biometric system to name a biometric subject's identity and its associated attributes. An example of an identifier would be a passport number.

Derived from National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

Identity

The set of attribute values (i.e. characteristics) by which a biometric subject is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that biometric subject from any other biometric subject and to distinguish the identity from any other identity.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Assurance

Operations that protect and defend identity information and management by ensuring their availability, integrity, authentication, confidentiality, intended use (privacy), and non-repudiation.

DoD Biometrics Strategy Working Group

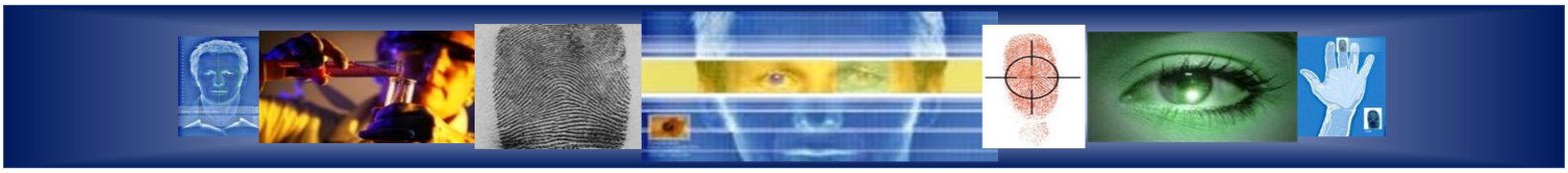
Identity Claim

A statement that a biometric subject is or is not the source of a reference in a database. Claims can be positive (I am in the database), negative (I am not in the database), or specific (I am end user 123 in the database).

Derived from NSTC Sub committee on Biometrics IAW INCITS/M1 and ISO/IEC JIYC 2 SC37standards bodies, Aug 2006.

Identity Dominance

The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity, or counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of a biometric subject and to establish a knowledge base for that identity.



Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Governance

The combination of policies and actions taken to ensure enterprise-wide consistency, privacy protection and appropriate interoperability between individual identity management systems.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Identity Management

A business function that authenticates an individual to validate identity, DoD affiliation, and authorization of the credential holder. The centralized data repository delivers credentialing information and status for business functions within DoD for use as proof of identity and DoD affiliation is delivered by Identity Management.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Protection

The process of safeguarding and ensuring the identities of individuals, devices, applications, and services are not compromised.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Identity Protection and Management Senior Coordinating Group (IPMSCG)

A DoD-level group that provides the enterprise coordinating framework for identity protection and management elements and activities for individuals, devices, applications, and services and oversee the integration of DoD-wide policy, capabilities and strategy for managing physical and virtual identities.

DoD D 852I.AAE DoD BIOMETRICS PROGRAM

Identity Superiority

The management, protection and dominance of identity information for friendly, neutral or unknown, and adversary subject through the application of military operations and business functions.

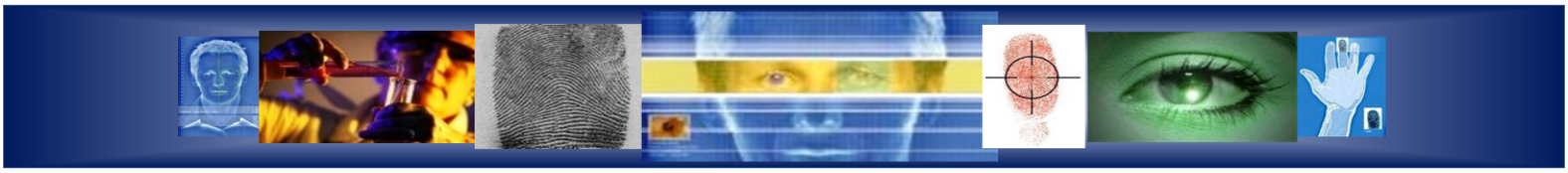
Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Integrated Automated Fingerprint Identification System (IAFIS)

The FBI's large-scale ten fingerprint (open-set) identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



Intermediate Biometric Sample Processing

Any manipulation of a biometric sample that does not produce biometric features. Example: Intermediate biometric samples may have been enhanced for biometric feature extraction.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

International Committee for Information Technology Standards (INCITS)

Organization that promotes the effective use of information and communication technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Interoperability

The conditions achieved among communications-electronic (CE) equipment systems or items of CE equipment when information or services can be exchanged directly and satisfactorily between them and their users.

Joint Publication 6-0, Joint Communication Systems, 20 March 2006

http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf

Iris Code©

A biometric feature format used in the Daugman iris recognition system.

National Science & Technology Council (NSTC), 14 September 06

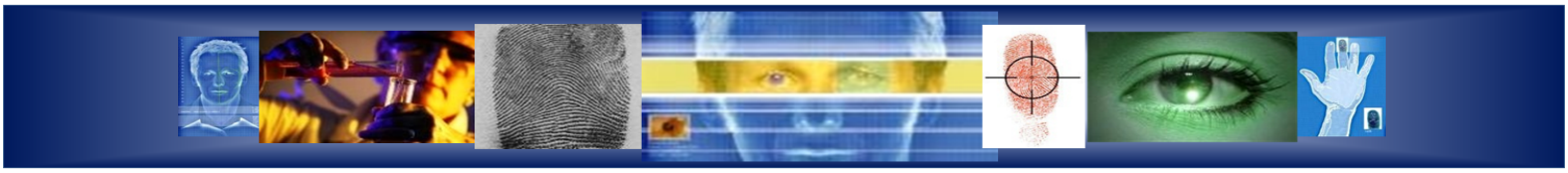
http://www.biometrics.gov/Documents/glossary.pdf

Iris Recognition

A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes. The iris muscle is the colored portion of the eye surrounding the pupil.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



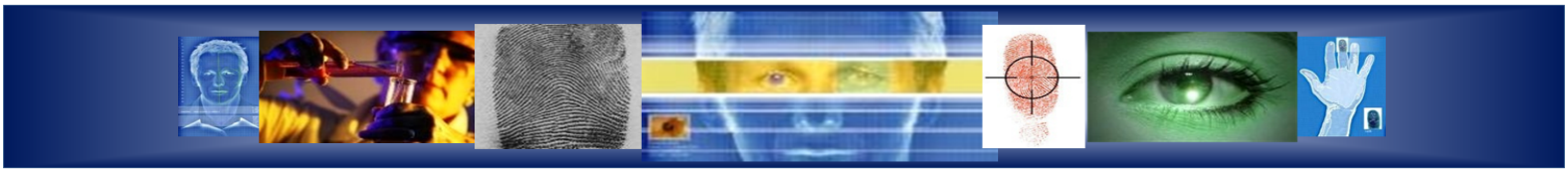
K

Keystroke Dynamics

A biometric modality that uses the cadence of a biometric subject's typing pattern for recognition.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



L

Latent Fingerprint

A fingerprint “image” left on a surface that was touched by a biometric subject. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Latent Sample

A biometric residue that is dormant, inactive, or non-evident but can be captured, measured and stored. It may be difficult to see, but can be made visible to scrutiny. A residue left on a medium that came in contact with a biometric subject.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Live Capture

Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface).

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Liveness Detection

A technique used to ensure that the biometric sample submitted is from a biometric subject. A liveness detection method can help protect the system against some types of spoofing attacks.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Live Scan

Occurs when taking a fingerprint or palm print directly from a biometric subject's hand.

Derived from ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

Locally Employed Personnel (LEP)

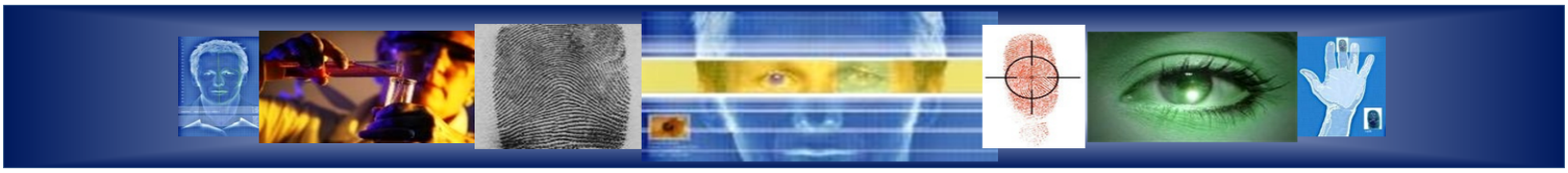
A person employed by the Coalition and US military, not US citizens.

USCENTCOM Biometric Identification System for Access (BISA) CONOPS

Local Trusted Source

A sub-set of the Authoritative Source and is established to accomplish a specific function within an operational mission or business process. Reasons for establishing a local trusted source might include: insufficient network connectivity to provide immediate access to the authoritative source, an operational need for closed-loop access, permission application.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006



Local Un-Trusted Source

A local repository of biometric files that that have not been enrolled with an authoritative or local trusted source. In many cases, local un-trusted sources are established for missions of short duration or to satisfy political, policy, or legal restrictions related to the sharing of biometric information.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Logical Access

Process of granting access to information system resources to authorized users, programs, processes, or other systems. The controls and protection mechanisms that limit users' access to information and restrict their forms of access to only what is appropriate.

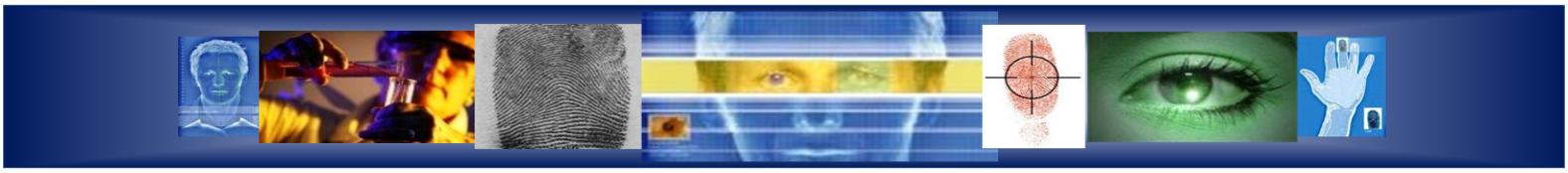
Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Loop

A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered. This pattern will contain one core and one delta.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



M

Match

The process of accurately identifying or verifying the identity of a biometric subject by comparing a standardized biometric file to an existing source of standardized biometric data, and scoring the level of confidence of the match. Matching consists of either a one-to-one (verification) or one-to-many (identification) search.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Minutia(e) Point

The point where a friction ridge begins, terminates, or splits into two or more ridges. Minutia(e) are friction ridge characteristics that are used to individualize a fingerprint image.

ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

Modality

A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Model

A representation used to characterize a biometric subject. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates.

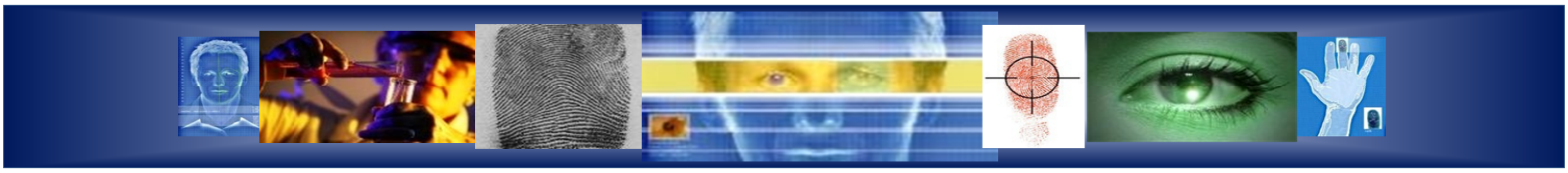
Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Multimodal Biometric System

A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006



N

National Institute of Standards and Technology (NIST)

A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's measurement and standards work promotes the well-being of the nation and helps improve, among many others things, the nation's homeland security.

National Institute of Standards and Technology

http://www.nist.gov/public_affairs/factsheet/homeland.htm

National Security Telecommunications and Information Systems Security Committee (NSTISSP #11)

National security community policy governing the acquisition of information assurance (IA) and IA-enabled information technology products.

The National Information Assurance Partnership, Common Criteria Evaluation Validated Scheme, Information Assurance Dictorate FAQ V2.1, 6 January 2002

http://www.niap-ccevs.org/cc-scheme/nstissp_11.pdf

Neutral or Unknown

Nonaligned individuals; host-country and third-country national non-US citizens.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Non-DoD Partners

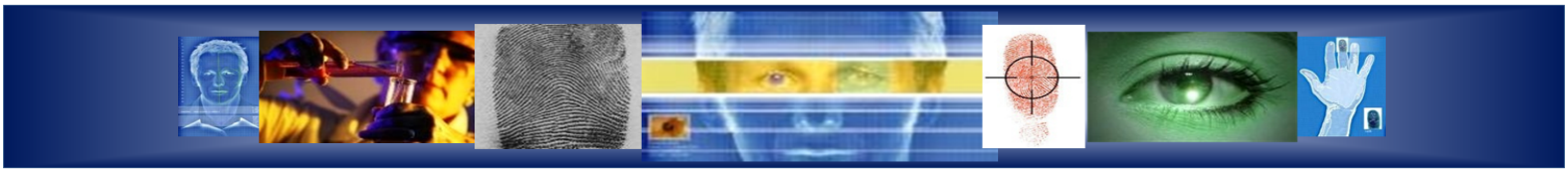
Interagency and Multinational partners

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Non-match

A decision that the recognition biometric sample(s) and the biometric reference are not from the same source.

JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007



O

One-to-Many

A phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. The phrase typically refers to the identification or watchlist tasks.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

One-to-One

A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one). The identification task can be accomplished by a series of one-to-one comparisons.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Open-set Identification

Biometric task that more closely follows operational biometric system conditions to 1) determine if a biometric subject is in a database and 2) find the record of the biometric subject in the database. This is sometimes referred to as the “watchlist” task to differentiate it from the more commonly referenced closed-set identification.

Derived from National Science & Technology Council (NSTC), 14 September 06

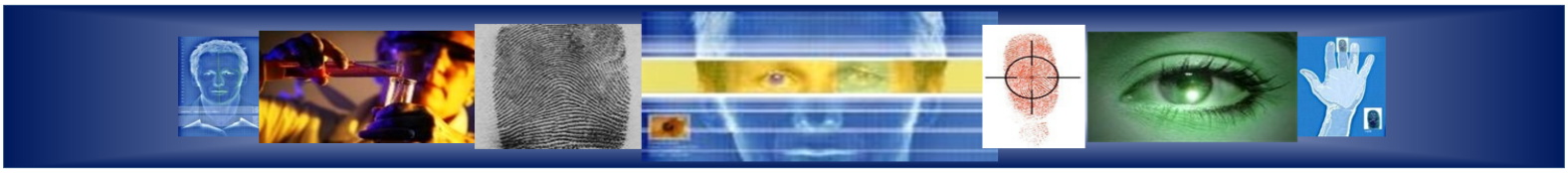
http://www.biometrics.gov/Documents/glossary.pdf

Operational Evaluation

One of the three types of performance evaluations. The primary goal of an operational evaluation is to determine the workflow impact seen by the addition of a biometric system.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



P

Palm Print Recognition

A biometric modality that uses the physical structure of a biometric subject's palm print for recognition purposes.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric algorithm or system.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Personal Identification Number (PIN)

A number used in conjunction with an access control system as a secondary credential by the user to ensure the holder of the access control card is the authorized user.

Naval Facilities Engineering Service Center , Antiterrorism Team website, Glossary of Terms

Person Data Exchange Standard (PDES)

A specification of the U.S. government intelligence community that specifies XML tagging of person data, including biometric data.

U.S. Government Person Data Exchange Standard (PDES)

Person of Interest

An individual for whom information needs or discovery objectives exist.

The DoD Biometrically-Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

Platen

The surface on which a finger is placed during optical finger image capture.

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

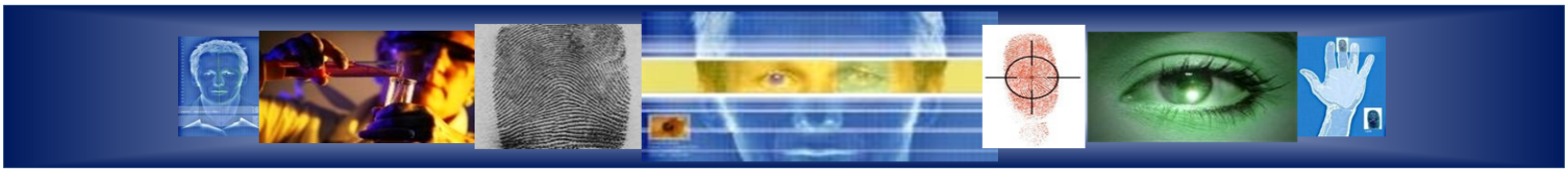
http://www.afb.org.uk/docs/glossary.htm

Probe

The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



R

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC compares false acceptance rate vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

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 the verification, closed-set identification or open-set identification (watchlist).

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Red Force

A collective term for enemy or opposing forces. It can include regular military, naval, and air forces as well as irregular combatant forces, terrorists, guerillas, and any other enemy combatant. A population group of individuals including, but not limited too, known enemy combatants, known or suspected terrorists, detainees, criminals, hostile foreign intelligence officers, and persons of interest.

DoD D 852I.AAE DoD BIOMETRICS PROGRAM

Re-enrollment

The process of establishing a new biometrics reference for a biometric subject already enrolled in the database.

JTC001-SC37-N-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

Reference (Function)

The process of querying various repositories of associated information on individuals (Intelligence, Medical, Human Resources, Financial, Security, Education, Law Enforcement, etc) for analysis purposes.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Response Time

The time used by a biometric system to return a decision on identification or verification of a biometric sample.

International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms

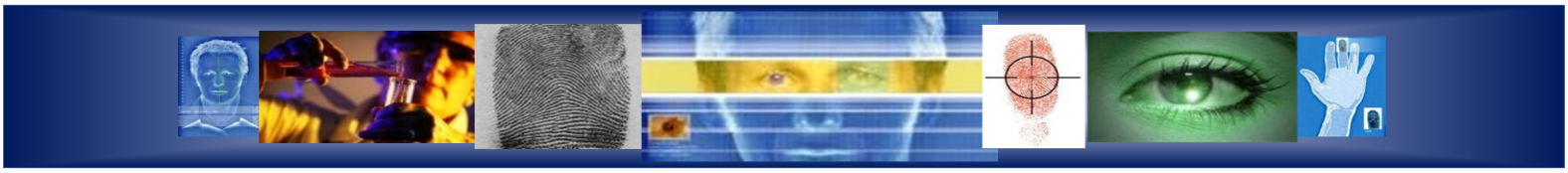
http://www.afb.org.uk/docs/glossary.htm

Ridge Ending

A minutiae point at the ending of a friction ridge.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

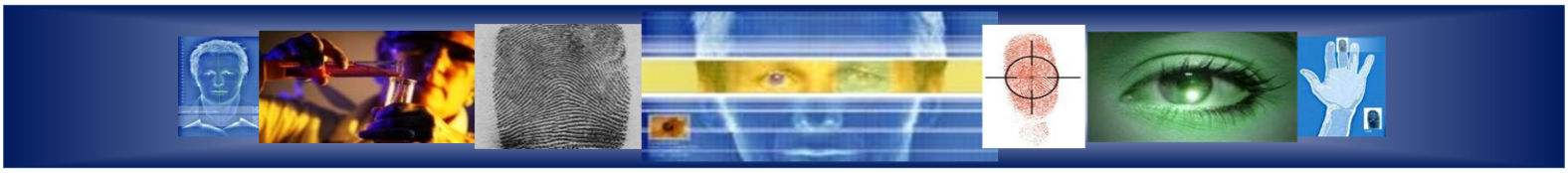


Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by “rolling” the finger across a sensor.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



S

Scenario Evaluation

One of the three types of performance evaluations. The primary goal of a scenario evaluation is to measure performance of a biometric system operating in a specific application.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Sensor

Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Share

Exchange standardized biometric files and match results among approved Army, DoD, Interagency, and Multinational partners in accordance with applicable law and policy.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Signature Dynamics

A behavioral biometric modality that analyzes dynamic characteristics of a biometric subject's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Similarity Score

A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Slap Fingerprint

Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card. Slaps are known as four finger simultaneous plain impressions.

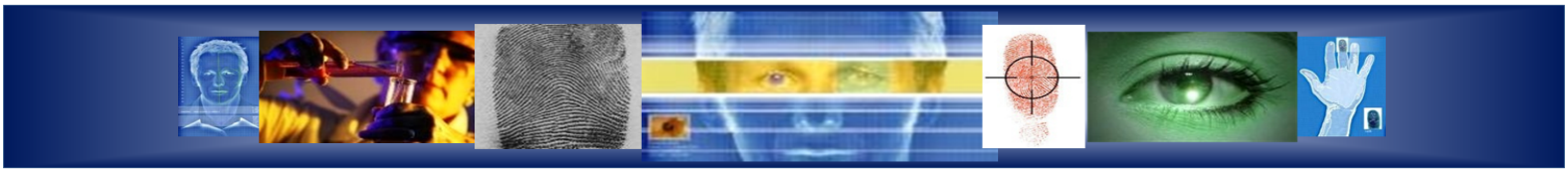
National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Source

An approved database and infrastructure that stores biometrics files.

Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006



Speaker Recognition

A biometric modality that uses a biometric subject's speech, a feature influenced by both the physical structure of a biometric subject's vocal tract and the behavioral characteristics of the biometric subject, for recognition purposes. Sometimes referred to as 'voice recognition.' 'Speaker Recognition' is not the same as 'Speech recognition' which recognizes the words being said and is not a biometric technology.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Speech Recognition

A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Spoofing

The ability to fool a biometric sensor into recognizing an illegitimate biometric subject as a legitimate biometric subject (Verification) or into missing an identification of someone that is in the database.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Store

The process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on biometric subjects when and where required. Biometric files are either enrolled or updated before they are stored.

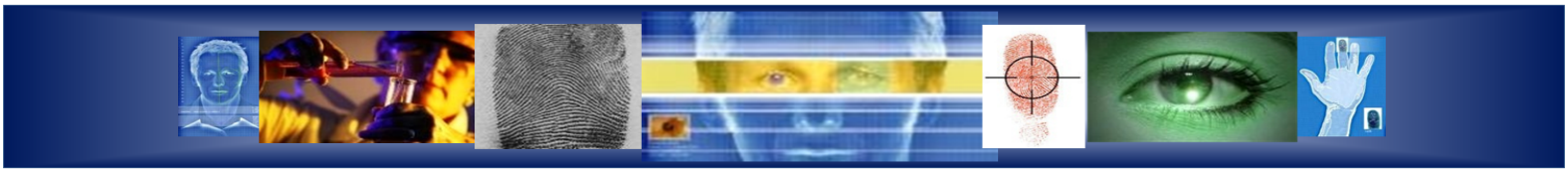
Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Submission

The process whereby a subject provides a biometric sample to a biometric system.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



T

Tactical Enrollment

Enrollment of biometric data on a subject that includes at least 2 fingerprints (indexes), 2 iris prints, and required text fields. The sample must be EBTS compliant. Typically used when subject is not being detained, but a record of the encounter is required at an ICED site, raid, humanitarian assistance, etc. It is an identification leading to an enrollment of a subject utilizing biometric data that includes at least 1 fingerprint or 1 iris and capture identification number. Used when subject is being detained and full enrollment will be conducted at the detention facility or at a base access point, when a subject is applying for a job on a base and is escorted to the LEP screening site for full enrollment.

Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

Template

A digital representation of a biometric subject's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison.

Derived from National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Tethered Biometric System

Use of biometric sensors between deployed personnel within a robust command and control architecture.

Biometrics Fusion Center

Threshold

A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Throughput Rate

The number of biometric transactions that a biometric system processes within a stated time interval.

National Science & Technology Council (NSTC), 14 September 06

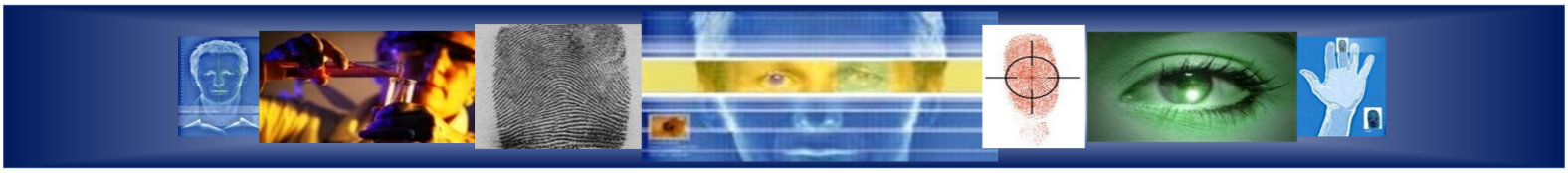
http://www.biometrics.gov/Documents/glossary.pdf

True Acceptance Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

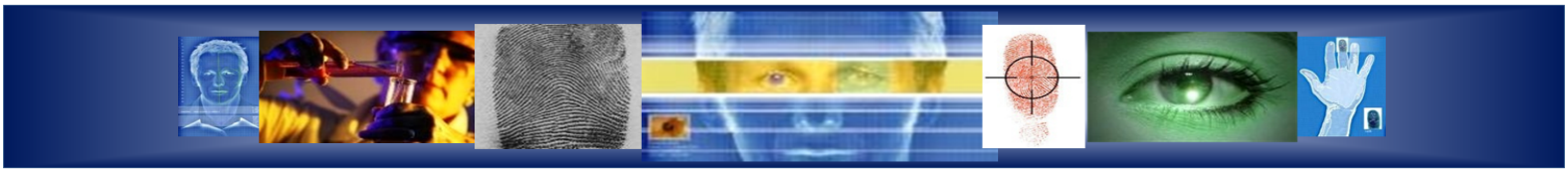


True Rejection Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



U

Untethered Biometric System

Collection, analysis and use of biometric sensors between deployed personnel outside of a robust command and control architecture.

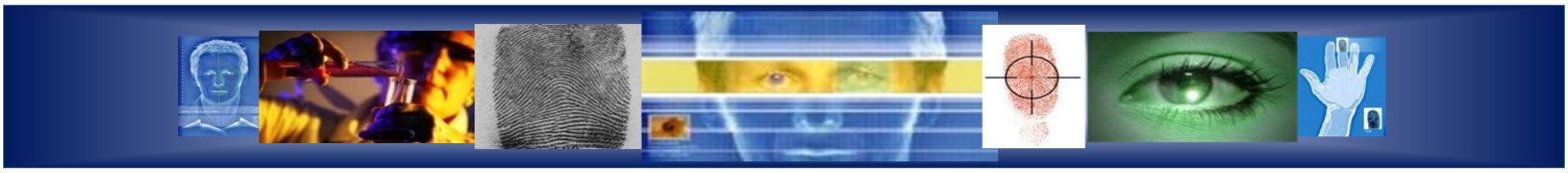
Biometrics Fusion Center

U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)

A continuum of security measures that begins overseas, at the Department of State's visa issuing posts, and continues through arrival and departure from the United States of America. Using biometrics, such as digital, inkless fingerscans and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the U.S. border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the U.S. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a known security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry and exit procedures address the U.S. critical need for tighter security and ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



V

Valley

The area of a fingerprint surrounding a friction ridge that does not make contact with an incident surface under normal touch; the area of the finger between two friction ridges.

ANSI INCITS 378-2004
Information technology - Finger Minutiae Format for Data Interchange

Verification

The one-to-one process of matching a biometric subject's biometric sample against his stored biometric file. Also known as Authentication.

Derived from Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

Verification Rate

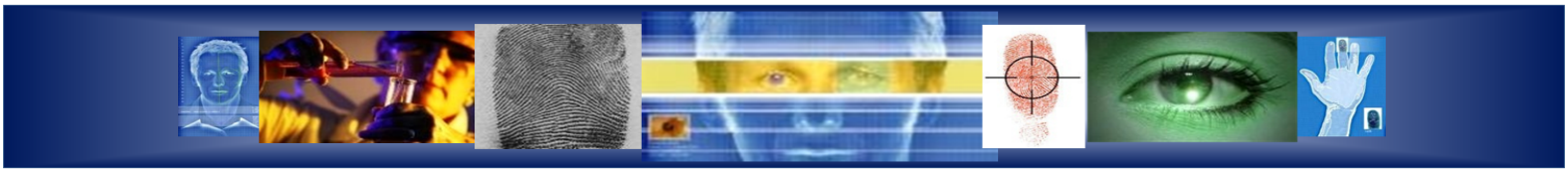
A statistic used to measure biometric performance when operating in the verification task. The rate at which legitimate biometric subjects are correctly verified.

Derived from National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

Vulnerability

The potential for the function of a biometric system to be compromised by intent (fraudulent activity), design flaw (including usage error), accident, hardware failure, or external environmental condition.

National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf



W

Watchlist

A term sometimes referred to as open-set identification that describes one of the three tasks that biometric systems perform. Answers the questions: Is this person in the database? If so, who are they? The biometric system determines if the individual's biometric template matches a biometric template of someone on the watchlist. The individual does not make an identity claim, and in some cases does not personally interact with the system whatsoever.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf

Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification (IAFIS-IC-0010 [V3])

Provides the definitions, requirements, and guidelines for specifying the FBI's WSQ compression algorithm. The document specifies the class of encoders required, decoder process, and coded representations for compressed image data.

Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification IAFIS-doc-01078-7.1

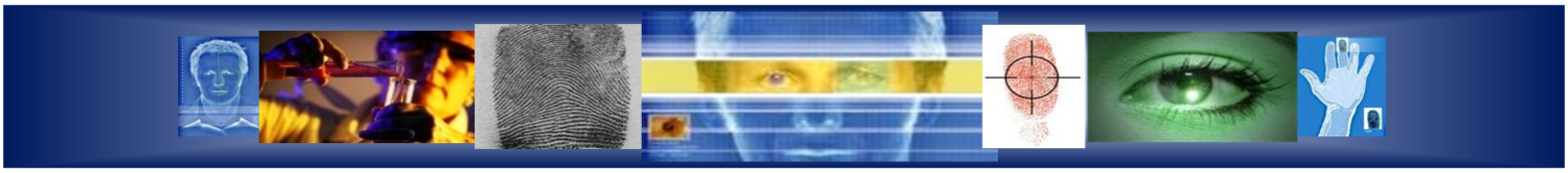
http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas.

National Science & Technology Council (NSTC), 14 September 06

http://www.biometrics.gov/Documents/glossary.pdf



Biometrics Glossary (BG)

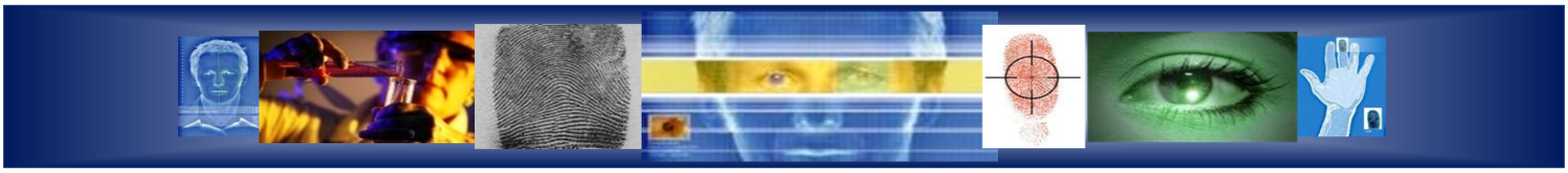
#

10 Print Match or Identification

An absolute positive identification of a biometric subject by corresponding each of his or her 10 fingerprints to those in a system of record. Usually performed by an AFIS system and verified by a human fingerprint examiner.

Derived from Biometrics Task Force

http://www.biometrics.dod.mil/ReferenceTutorials/BiometricsGlossary/tabid/87/Default.aspx



Biometrics Glossary (BG)

References

1 ANSI INCITS 378-2004
Information technology - Finger Minutiae Format for Data Interchange

2 ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information
http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

3 Biometric Intelligence Resource (BIR) Implementation: 2006-2007
BIR Version 2 System Design Document (SDD) 20 June 2007

4 Biometrics Fusion Center

5 Biometrics Task Force
http://www.biometrics.dod.mil/ReferenceTutorials/BiometricsGlossary/tabid/87/Default.aspx

6 Biometrics Task Force And Navy Team for Success January 2007

7 Biometrics Task Force & Biometrics Data Team

8 Biometrics Task Force Strategy Division

9 Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

10 Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification IAFIS-doc-01078-7.1
http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf

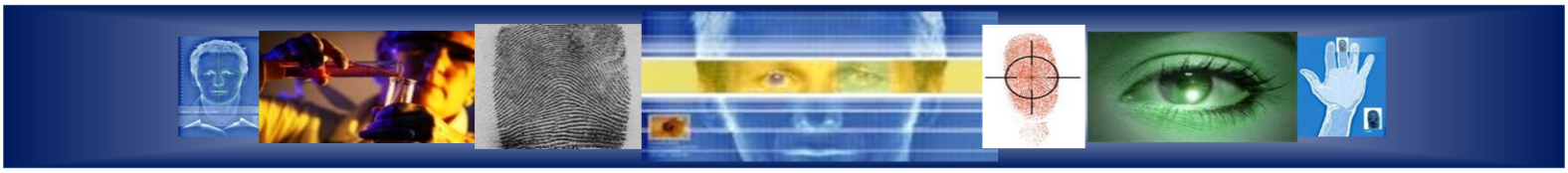
11 Defense Biometric Identification System User Manual, May 24, 2006

12 Department of Defense
Electronic Biometric Transmission Specification
23 August 2005 Version 1.1 DIN: DOD_BMO_TS_EBTS_Aug05_01.01

13 Detainee Reporting System courtesy of National Detainee Reporting Center, August 06

14 DoD Biometrics Strategy Working Group

15 DoD D 852I.AAE DoD BIOMETRICS PROGRAM



Biometrics Glossary (BG)

References

16 DoD Deputy Secretary of Defense Memorandum, Smart Card Adoption and Implementation, 10 November 1999

17 Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints
http://www.fbi.gov/hq/cjisd/takingfps.html

18 Initial Capabilities Document (ICD) for Biometrics in Support of Personnel Identity (BSPI) (Draft), 30 Jun 07

19 International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), 1999 Glossary of Biometric Terms
http://www.afb.org.uk/docs/glossary.htm

20 Joint Publication 3-0, Joint Operations,17 September 2006
http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf

21 Joint Publication 6-0, Joint Communication Systems, 20 March 2006
http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf

22 JTC001-SC37-n-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

23 JTC001-SC37-N-2263 Text of Standing Document 2(SD2) Version 8, Harmonized Biometric Vocabulary, November 2007

24 National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003, Sponsored by the DoD Biometrics Management Office (BMO) and the National Security Agency (NSA)

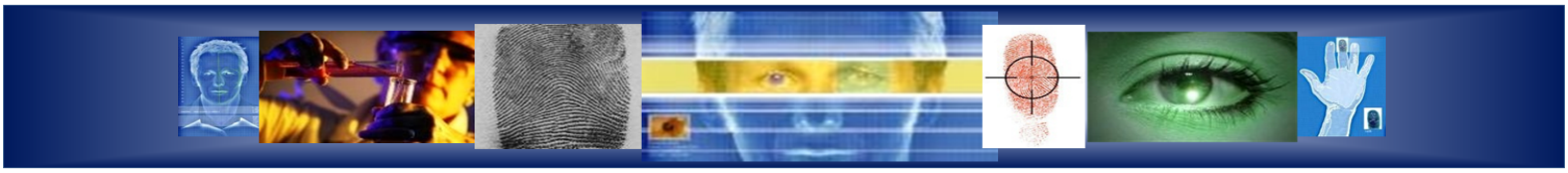
25 National Institute of Standards and Technology
http://www.nist.gov/public_affairs/factsheet/homeland.htm

26 National Institute of Standards and Technology Interagency Report (NISTIR) 6529-2001, Common Biometric Exchange File Format, 3 January 2001

27 National Science & Technology Council (NSTC), 14 September 06
http://www.biometrics.gov/Documents/glossary.pdf

28 Naval Facilities Engineering Service Center , Antiterrorism Team website, Glossary of Terms

29 NSTC Sub committee on Biometrics IAW INCITS/M1 and ISO/IEC JIYC 2 SC37standards bodies, Aug 2006.



Biometrics Glossary (BG)

References

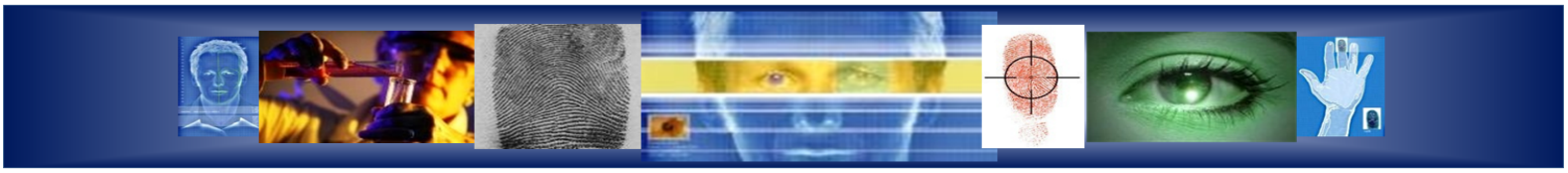
30 The DoD Biometrically-Enabled Watchlist (BEWL) A Federated Approach, May 3, 2007

31 The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines . Version 1.03, September 2003
http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf

32 The National Information Assurance Partnership, Common Criteria Evaluation Validated Scheme, Information Assurance Dictorate FAQ V2.1, 6 January 2002
http://www.niap-ccevs.org/cc-scheme/nstissp_11.pdf

33 USCENTCOM Biometric Identification System for Access (BISA) CONOPS

34 U.S. Government Person Data Exchange Standard (PDES)



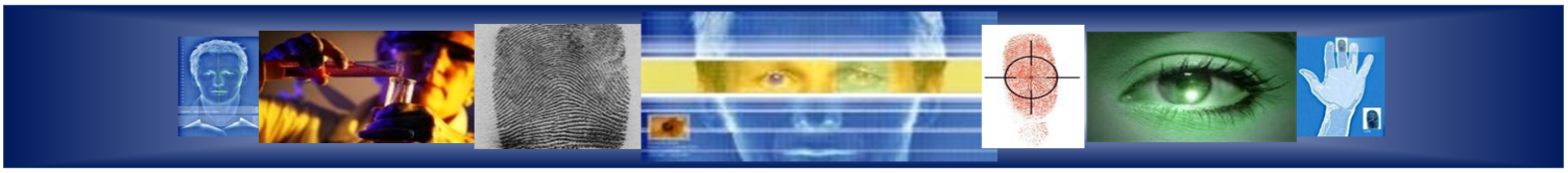
Version 1.0

Biometrics Glossary (BG)

Feb 1, 2008

Acronyms

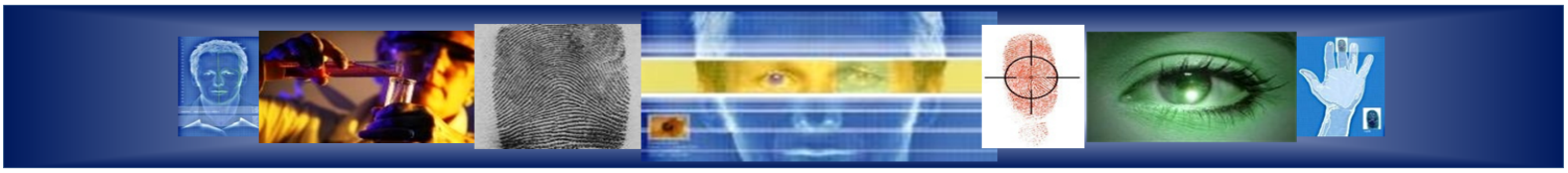
ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AIMS	Automated Identification Management System
ANSI	American National Standards Institute
AOR	Area of Responsibility
ASCII	American Standard Code for Information Interchange
BAT	Biometric Automated Toolset
BC	Biometric Consortium
BDT	Biometric Data Team
BFC	Biometric Fusion Center
BIAR	Biometric Intelligence Analysis Report
Bio API	Biometric Application Programming Interface
BIR	Biometric Information Record
BIR	Biometric Intelligence Resource
BISA	Biometric Identification System for Access
BMO	Biometric Management Office
BSWG	Biometric Standards Working Group
BTF	Biometric Task Force
CAC	Common Access Card
CBA	Capabilities Based Assessment
CBEFF	Common Biometric Exchange File Format
CBEFF	Common Biometric Exchange Formats Framework
CE	Communications Equipment
CENTCOM	Central Command
CJIS	Criminal Justice Information Services
CMC	Cumulative Match Characteristic
CMR	Cumulative Match Rate
CONOPS	Concept of Operations



Biometrics Glossary (BG)

Acronyms

DBEKS	DoD Biometric Expert Knowledgebase System
DBIDS	Defense Biometric Identification System
DET	Detection Error Trade off
DMDC	Defense Manpower Data Center
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DPI	Dots Per Inch
DRS	Detainee Reporting System
EBTS	Electronic Biometric Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification
EMIO	Expanded Maritime Interdiction Operations (NAVY)
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FHA	Foreign Humanitarian Assistance
FMR	False Match Rate
FNMR	False Non Match Rate
FOUO	For Official Use Only
FP	Force Protection
FpVTE	Fingerprint Vendor Technology Evaluation
FRR	False Rejection Rate
FRVT	Face Recognition Vendor Test
FTA	Failure To Acquire
FTE	Failure To Enroll
GMM	Gaussian Mixture Model
HD	Hamming Distance
HMM	Hidden Markov Model
IAFIS	Integrated Automated Fingerprint Identification System



Biometrics Glossary (BG)

Acronyms

IBDD	Integrated Biometric Data Dictionary
IDS_MD	Identity Dominance System - Maritime Domain
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
JTC	Joint Technical Committee
LDM	Logical Data Model
LEP	Locally Employed Personnel
NGIC	National Ground Intelligence Center
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
ORCON	Dessemination & Extraction of Information Controlled by Originator
POI	Person(s) of Interest
PPI	Pixels Per Inch
RAPID	Real-time Automated Personnel Identification System
RFS	Ready For Staffing
ROC	Receiver Operating Characteristics
SCI	Sensitive Compartmented Information
SME	Subject Matter Expert
SWGFAST	Scientific Working Group on Friction Ridge Analysis, Study and Technology
TS	Top Secret
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language