Biometrics Glossary (BG)

01 August 2008
Release 2.0

Prepared for:
United States Army
Biometrics Task Force

Prepared by:
Software Engineering Center
CECOM Life Cycle Management Command

Biometrics Glossary (BG)

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

Convert 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

Biometrics Glossary (BG)

A

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

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

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.

Derived from 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

B

BECC

This system will be Next Generation ABIS, which will be known as the Biometrics Enterprise Core Capabilities (BECC), which will be a comprehensive system, the requirements will be based on, multi-modal, multi-functional and includes multi-domain biometrics collection, storage, and matching Pursuant to this effort.

CAPABILITY PRODUCTION DOCUMENT FOR Biometric Enterprise Core Capabilities (BECC), Version 2.0, 14 January 2008

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 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

B

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.

Derived from 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.

Derived from 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

B

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 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. The biometric file is composed of the biometric sample(s) and contextual data (biographic data and situational information.)

Derived from 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.

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

B

Biometric Intelligence Analysis Report (BIAR)

BIARS are first phase analytical products that provide current intelligence assessments on individuals who have been biometrically identified at least once and who may pose a threat to US interests. BIARS provide a summary and background on a person's biometric encounters, all-source intelligence analysis, assessments of the subject's threat and intelligence value, summary of actions taken by the analytical element and recommended actions for operators.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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 Model

Stored function (dependent on the biometric data subject) generated from a biometric feature(s).

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

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

Biometrics Glossary (BG)

B

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.

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

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

Biometric Sample

Data that represents a biometric characteristic of a biometric subject as captured by a biometric system. A Biometric sample is an integral component of the biometric file.

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

Biometric Sample Collector

An individual performing the biometric sample collection.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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-enabled Intelligence

Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist / insurgent network and related pattern analysis, facilitates high value individual targeting, reveals movement patterns, and confirms claimed identity.

DoD D 8521.01E DoD BIOMETRICS PROGRAM

http://www.biometrics.dod.mil

Biometrics Enterprise

The Biometrics Enterprise is an entity comprised of the Department's joint, Service, and Agency organizations working together to integrate biometrics into the identity transactions needed to support military operations and departmental business functions.

Department of Defense Biometrics Enterprise Strategic Plan, 2008-2015, Final Draft, June 12, 2008

B

Biometrics Program

All systems, interfaces, acquisition programs, processes, and activities that are utilized to establish identities of people through the use of biometrics modalities.

DoD D 8521.01E DoD BIOMETRICS PROGRAM

http://www.biometrics.dod.mil

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.
NOTE 1: A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced
or compressed form, is not a biometric template.
NOTE 2: The biometric features are not considered to be a biometric template unless they are stored for reference.

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

C

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 sample and related contextual data from a biometric subject, with or without his knowledge.

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

Common Biometric Exchange Formats Framework (CBEFF) specification

A set of data elements for use in biometric record headers that supports the interchange of biometric data.

National Institute of Standards and Technology Interagency Report (NISTIR) 6529-A, Common Biometric Exchange Formats Framework, 5 April 2004

http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf

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

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

C

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.

Derived from 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.

Derived from 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

Deoxyribonucleic acid (DNA) Matching

Utilizing DNA to identify a biometric subject.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

Detainee Reporting System (DRS)

A System designed to support the processing of prisoner of war (POWs) and detainees.

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

Biometrics Glossary (BG)

D

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

Exemplar

Friction ridge record of an individual, recorded electronically, photographically, by ink or other medium.

Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Glossary - Consolidated (9/9/03 ver. 1.0)

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

Biometrics Glossary (BG)

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

False Acceptance

When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates a biometric subject 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 sample. 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 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

F

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 a 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

F

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

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

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

Biometrics Glossary (BG)

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

Biometrics Glossary (BG)

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

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)

Identitity Facilitation

The capability to plan, organize, lead, coordinate, and control the use of resources to deliver accurate, complete, secure, and timely identity information products and services to operational users on demand.

Functional Area Analysis (FAA), Biometrics Support to Identity Management, 21 August 2007

Identitity Integration

Identity Integration highlights the capability of Services, COCOMs, government agencies, international and national organizations, and associated systems, resources, and entities to cooperate and interoperate as needed to deliver Identity Assurance, Identity Protection, and Identity Facilitation products and services to support warfighter/user operations.

Functional Area Analysis (FAA), Biometrics Support to Identity Management, 21 August 2007

Identity

The set of attribute values (i.e. characteristics) by which a biometric subject is recognizable 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

I

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 to 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. This includes denying an adversary the ability to discover our protected assets.

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

Identity Management

A business function that authenticates a biometric subject to validate identity, DOD affiliation, and authorization of the biometric subject. Comprised of Identity Assurance, Identity Dominance, Identity Protection, Identity Facilitation and Identity Integration.

Derived from Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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

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

I

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

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.

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

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

K

Keystroke Dynamics

A potential 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 Print

Transferred impression of friction ridge detail not readily visible; generic term used for questioned friction ridge detail.

Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Glossary - Consolidated (9/9/03 ver. 1.0)

Latent Sample

A biometric residue that is dormant, inactive, or non-evident but can be captured, measured and stored.

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

Live Capture

Fingerprint capture technique 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).

Derived from 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 living biometric subject.

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 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

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

L

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

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

Comparison decision that the recognition biometric sample(s) and the biometric reference are from the same source.

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

Mimic

The presentation of a biometric sample in an attempt to fraudulently impersonate someone other than the biometric subject.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

http://fingerprint.nist.gov/standard/Approved-Std-20070427.pdf

Modality

A type or class of biometric sample originating from a biometric subject. For example: face recognition, fingerprint recognition, iris recognition, DNA, etc.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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

Non-match

Comparison 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

Comparing one biometric reference to many biometric references to identify a biometric subject. Sometimes referred to as 1: n.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

One-to-One

Comparing one biometric reference to another biometric reference to identify a biometric subject.

Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

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

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

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

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

Re-enrollment

The process of establishing a new biometrics reference for a biometric subject already enrolled in the database.
NOTE 1: Re-enrolment requires new captured biometric sample(s).

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

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

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 DoD, Interagency, and Multinational partners in accordance with applicable law and policy.

DoDD 8521.01E DoD Biometrics Program

http://www.biometrics.dod.mil

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

Situational Information

The who, what, when, where, how, why, etc. associated with a collection event and permanently recorded as an integral component of contextual data.

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

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

S

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

Store

The process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric information on biometric subjects when and where required.

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 IED 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

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

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

W

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

Biometrics Glossary (BG)

References

Biometrics Fusion Center

Biometrics Task Force

Biometrics Task Force And Navy Team for Success January 2007

Biometrics Task Force & Biometrics Data Team

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

Defense Biometric Identification System User Manual, May 24, 2006

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

DoD Biometrics Strategy Working Group

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

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

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

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)

National Institute of Standards and Technology

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

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

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

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

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

Biometrics Glossary (BG)

References

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

USCENTCOM Biometric Identification System for Access (BISA) CONOPS

USCENTCOM Biometric Identification System for Access (BISA) CONOPS

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

Biometrics Glossary (BG)

Acronyms

Acronym	Definition
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
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

Biometrics Glossary (BG)

Acronyms

Acronym	Definition
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
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

Biometrics Glossary (BG)

Acronyms

Acronym	Definition
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