BIMA
BIOMETRICS IDENTITY MANAGEMENT AGENCY

Biometrics Glossary

Version 6.0

April 2012

Prepared by:
Software Engineering Center
CECOM Life Cycle Management
Command

Biometrics Glossary Introduction

Background

The Department of Defense (DoD) Biometrics Enterprise comprises the Department's joint service, and agency organizations working together to integrate biometrics into the transactions needed to support military operations and business functions. It is envisioned to be a flexible, global biometrics enterprise that protects individuals' rights, enables services for our personnel, friends and partners, and denies anonymity to adversaries. It is also envisioned to be a flexible service that is able to continuously adapt to changing business processes and military missions.

As the DoD Biometrics Enterprise has evolved, so has the vocabulary used to describe the various concepts inherent in the military missions and business functions. However, during this evolution terminology was inconsistently developed, used and defined, thereby creating confusion, inconsistency, and imprecision when clarity, consistency and accuracy was needed. It became apparent an authoritative source for DoD biometrics terminology was needed resulting in the development of the Biometrics Glossary (BG). Since language does not remain static -- new terms are created, existing terms are modified and refined over time, and occasionally some are retired when they become deprecated or obsolete -- accommodating the natural evolution of language is a prime concern for the BG to remain relevant.

Purpose

The purpose of the BG is to compile and present a common, "standardized" business language of biometric terms from authoritative sources. This glossary will promote a common lexicon for DoD stakeholders to reference and use in the development and updating of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF), and in communication with other U.S. Government and International stakeholders.

Scope

The scope of the BG is to provide definitions for the conceptual and operational terms commonly used in biometrics discussions and formal documents such as DoD Directives, CONOPS, and materials required in the JCIDS process. The BG does not include technical biometrics terms or other DoD terminology that is not biometrics-specific.

The BG differs from the Integrated Data Dictionary (IDD) in that the latter focuses on the specific data fields that are exchanged among biometric systems, and their individual characteristics (e.g. field size, datatype, etc.). The IDD addresses biometric information at a much lower and more detailed level than the BG. Together the Glossary and IDD are comprehensive recordings of the biometrics vocabulary from both the business and machine-to- machine communications perspectives. The BG may be used as input to the AV-2 Integrated Dictionary, one of the requisite data artifacts within the DoD Architecture Framework (DoDAF) v1.5 and v2.0.

Sources

The BG was developed by consolidating existing DoD glossary material and incorporating terms from other authoritative sources. A complete listing of all sources used in this BG is listed in the References section.

Hierarchy

When a term is found to have been defined differently in two or more sources, as a general rule the BG definition is to be taken from the source ranked highest in the source hierarchy that has been established by the BIMA. In cases where a lower-level reference is better suited in defining the biometric term, the lower level source may be used.

Top-level authoritative references to be used to determine which definition will be included in this BG are as follows:

- DoD Directive 8521.01E DoD BIOMETRICS PROGRAM
- Biometrics in Support of Identity Management Joint Capabilities Document
- DoD Joint Publications
- JTC001-SC37-n-2263 Text of Standing Document, Harmonized Biometric Vocabulary
- National Science & Technology Council (NSTC)
- Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
- Department of Defense Electronic Biometric Transmission Specification (EBTS) v1.2, v2.0, & v3.0
- ANSI/NIST-ITL 1-2011. American National Standard for Information Systems Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
- Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints
- Biometrics Identity Management Agency
- Other sources

Business Rules

The BG will attempt to provide one definition per term, but may have more than one definition per term based on usage/discipline. Terms will be definitive to DoD Biometrics, but will maintain an international approach if determined by the references above. When a term is first defined in a BIMA-produced document the BIMA will be the authoritative author. The BG will address DoD Biometrics terms related to Policy, Operational Techniques, Tactics and Procedures (TTP) and important technical distinctions with existing DoD Policy and/or TTP. Website entries will be authoritative to USG and international as determined by the sources above. Glossary entries should be enduring and not be readily subject to change except as necessary to support stakeholder needs or changes to source documents.

Intended Audience

The intended audience for the BG is a wide one that spans representatives from the DoD Biometrics Community tasked with writing and/or reviewing formal and technical documents from military operations and business functions perspectives to the general reader seeking to expand his/her knowledge of biometrics in the DoD.

Term Elements

The BG will contain the following elements for each term:

Term Name – Conceptual and operational terms commonly used in biometrics discussions and formal documents such as DoD Directives, CONOPS and materials required in the JCIDS process.

Description – Definition for the term name.

Reference – Authoritative source(s) used to define the term name and definition. Where available, a hyperlink to the source will be provided.

See Also – Where found, the "*See Also*" reference will inform readers of terms in the BG that may also be of interest based on the current term. This is a discovery aid to leverage information in the BG not evident because of the Glossary's alphabetical organization. A root term will reference associated terms of interest; each of those will lead back to only the root term.

Change Control

The Biometrics Glossary Change and Revision Control Process establishes the process by which changes to the BG are to be proposed, discussed, reviewed, accepted, and implemented. It will ensure that consistent change control management procedures accommodate:

1. BG Change Request (CR) tracking from initiation to closure
2. Communication of CR status among BG stakeholders
3. Implementation of the approved changes to the BG
4. BG revision control and circulation of the new versions
5. Archiving CRs, meeting minutes and previous BG versions

Statistics

The Biometrics Glossary Version 6.0 (April 2012) contains 224 terms from 69 sources. The Acronym List contains 117 acronyms. Changes to terms from version 5.0 include:

Added – 19
Modified – 31
Sunsetted – 1
Retired – 0

A detailed summary of all changes can be found in the *Biometrics Glossary Version Delta V6.0 to V5.0*.

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 2006 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. See Also: DoD Biometrics Process. Derived From: Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
ANSI/NIST-ITL	This standard defines the content, format, and units of measurement for the electronic exchange of fingerprint, palmprint, plantar, facial/mugshot, scar, mark & tattoo (SMT), iris, deoxyribonucleic acid (DNA), and other biometric sample and forensic information that may be used in the identification or verification process of a subject. Derived From: ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136
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. See Also: Fingerprint. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

A

Armed Forces DNA Identification Laboratory (AFDIL)	A division of the Office of the Armed Forces Medical Examiner under the Armed Forces Institute of Pathology. Provides scientific consultation, research and education services in the field of forensic DNA analysis to the Department of Defense and other agencies, as well as worldwide, and DNA reference specimen collection, accession, and storage of United States military and other authorized personnel.
	Armed Forces DNA Identification Laboratory website
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 2006 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

A

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)
Automated Biometric Identification System (ABIS)	See: AFIS, IAFIS, DoD ABIS, IDENT.
	Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil
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 2006 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 Identity Management Agency (BIMA) 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

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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Bifurcation	The point in a fingerprint where a friction ridge divides or splits to form two ridges. See Also: Fingerprint. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Binning	The process of parsing or classifying data in order to accelerate and/or improve biometric matching. Derived From: National Science & Technology Council (NSTC), 14 September 2006 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

B

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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Biometric	Of or having to do with biometrics. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Biometric Analysis Packet (BAP)	A Biometrics-enabled Intelligence (BEI) product that provides identities of personnel who are biometrically enrolled or watch listed for a specified location. The BAP also provides a brief background summary of the personalities associated with the individual. See Also: BEI Derived From: Handbook No. 11-25. Commanders Guide to Biometrics in Afghanistan. April 2011
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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

B

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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Biometric Capture Process	Process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Biometric Characteristic	A biological and/or 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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

B

Biometric Data	A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations. DoD Directive 8521.01E Enclosure 2 http://www.biometrics.dod.mil
Biometric Data Block	A block of data with a defined format that contains one or more biometric samples or biometric templates. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Biometric Encounter	A biometric encounter occurs when a biometric sample(s) is captured from an individual or a latent biometric sample(s) is collected. Derived From: The DOD Biometrically-enabled Watchlist (BEWL), A Revised Federated Approach, August 2009

B

Biometric Feature	Numbers or labels extracted from biometric samples and used for comparison. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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 that contains an open-set or closed-set identification application. See Also: Open-set Identification, Closed-set Identification JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

B

Biometric Identification System for Access (BISA)	A biometric and contextual data collection and credential card production system. Derived From: Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
Biometric Identity	A biometric identity is established when a biometric sample(s) is used instead of a name to identify a Person of Interest (POI). The biometric identity may consist of the results of one or more biometric encounters for the same individual. Derived From: The DOD Biometrically-enabled Watchlist (BEWL), A Revised Federated Approach, August 2009
Biometric Identity Intelligence Resource (BI2R)	Automated database that stores biometric and associated intelligence data from DoD collection devices. Analysts use the BI2R toolset to conduct analysis and develop intelligence reports supporting DoD and national missions. The system is designed to provide the DoD, IC, and coalition communities with authoritative, high pedigree, biometrically base-lined identities, and advanced tools and technologies necessary to analyze, collaborate, produce, disseminate, and share biometric identity intelligence. See Also: AIMS, BIR Derived From: TC 2-22.82 Biometrics-Enabled Intelligence March 2011
Biometric Information	A catch all phrase that includes but is not limited to biometric data, contextual data and associated information obtained during the biometric process. Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil

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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

B

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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Biometric Record	Data record containing biometric data. Note: A biometric record may include non-biometric data.
	JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

B

Biometric Sample	Analog or digital representation of biometric characteristics, or biological specimen prior to biometric feature extraction. Derived From: JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Biometric Sample Collector	An individual performing the biometric sample collection. Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008
Biometric Standards	Biometric Standards are agreed upon formats established by the DoD internal as well as external authoritative agencies, that provide rules, guidelines, and characteristics for biometric activities and their results. Interoperability is facilitated by the standards as they establish the size, configuration, or protocol of biometric products, processes, and systems. Biometric Standards specify: 1. Formats for the interchange of biometric data. 2. Common files format that provide platform independence and separation of transfer syntax from content definition. 3. Application program interfaces and application profiles. 4. Performance metric definitions and calculations. 5. Approaches to test performance. 6. Requirements for reporting the results of performance tests. Derived From: National Science and Technology Council (NSTC): Biometric Standards http://www.biometrics.gov/Documents/biostandards.pdf
Biometric Subject	An individual from which biometric samples were collected. Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil

B

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 2006 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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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 Revised Federated Approach, August 2009
Biometrics	A general term used alternatively to describe a characteristic or a process. As a characteristic: The measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) and/or behavioral biometric characteristics.
	Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Biometrics Application Programming Interface (Bio API)	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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Biometrics Enabling Capability (BEC)	This system will be the Next Generation ABIS, which will be known as the Biometrics Enabling Capability (BEC). The BEC will be a comprehensive system with requirements based on multi-modal, multi-functional and multi-domain biometrics collection, storage, and matching pursuant to this effort.
	Derived From: Capability Production Document For Biometric Enterprise Core Capabilities (BECC), Version 2.0, 14 January 2008 and DoD Biometrics Overarching Integrated Product Team (OIPT) Report, April 8, 2010

B

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
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 Directive 8521.01E Enclosure 2 http://www.biometrics.dod.mil
Biometrics-Enabled Intelligence (BEI)	Intelligence resulting from the collection, processing, analysis, and interpretation of biometric signatures; the contextual data associated with those signatures; and other available intelligence that answers a commander's or other decision-maker's information needs concerning persons, networks, or populations of interest. See Also: BI2R
	Initial Capabilities Document for Biometrics Enabled Intelligence (BEI). Version 1.0 26 February 2010

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.). See Also: Verification, Biometric Identification Application, Open-set Identification Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Collect	The capability and/or process to capture biometric sample(s) and related contextual data from a biometric subject, with or without his or her knowledge. See Also: DoD Biometrics Process. Derived From: Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
Combined DNA Index System (CODIS)	Both a program and software tool used by the FBI, distributed over three hierarchical levels – National, State and Local Index Systems – that enables state and local law enforcement crime laboratories to exchange and compare DNA profiles electronically. Federal Bureau of Investigation (FBI) website, National DNA Index System http://www.fbi.gov/about-us/lab/codis
Common Biometric Exchange Formats Framework specification (CBEFF)	This standard specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications. This standard specifies the biometric data elements. Common Biometric Exchange Formats Framework (CBEFF), ANSI INCITS 398-2008 http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+INCITS+398-2008

C

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 2006 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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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
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. See Also: Fingerprint. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

C

Covert Collection	Collection of biometrics without the knowledge of an individual. An instance in which biometric samples are being collected at a place and/or time that is not known to the bystanders. An example of a covert environment might involve an airport checkpoint where facial images of passengers are captured and compared to a watchlist without their knowledge. See Also: Overt Collection Derived From: National Science and Technology Council (NSTC), 27 July 2006 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 2006 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. See Also: DoD Biometrics Process.
	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 2006 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. See Also: Fingerprint.
	National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

D

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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Detection Error Trade-off Curve (DET)	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 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf
DNA Matching	Utilizing DNA to identify a biometric subject. See Also: Modality. Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008

D

DNA Profile	A set of DNA identification characteristics resulting from DNA analysis.The digital representation of a nuclear DNA profile is used for automated biometric comparison. The data in a DNA profile cannot be analyzed to reveal sensitive personal or medical information about the individual the DNA was obtained from. Also referred to as "DNA Type".
	Chemical Science and Technology Laboratory/NIST website, Quality Assurance Standards for DNA Testing Laboratories http://www.cstl.nist.gov/strbase/QAS/Final-FBI-Director-Forensic-Standards.pdf
DNA Record	The DNA profile and operational identifiers such as agency identifier, specimen identification number, and name of the participating laboratory and personnel associated with DNA profile analyses. Records in the database do not include DNA samples or classified information.
	Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil
DNA Sample	A collection of DNA molecules that can be quantified, amplified, separated, and analyzed.
	State of the Art Biometrics Excellence Roadmap Technology Assessment: Volume 3 DNA, March 2009
DNA Source	The individual or material from which a DNA sample can be collected or extracted.
	State of the Art Biometrics Excellence Roadmap Technology Assessment: Volume 3 DNA, March 2009

D

DNA Template	Previously existing DNA on which new DNA is synthesized. "DNA Template" is not the same as "Biometric Template" and does not have a biometric usage.
	Microbiology Procedure website http://www.microbiologyprocedure.com/replication-of-DNA/template-DNA.htm
DNA Type	See DNA Profile.
	Chemical Science and Technology Laboratory/NIST website, Quality Assurance Standards for DNA Testing Laboratories http://www.cstl.nist.gov/strbase/QAS/Final-FBI-Director-Forensic-Standards.pdf
DoD Automated Biometric Identification System (DoD ABIS)	DoD ABIS is the central, authoritative, multi-modal biometric data repository. The system operates and enhances associated search and retrieval services and interfaces with existing DoD and interagency biometrics systems. The repository interfaces with collection systems, intelligence systems and other deployed biometric repositories across the federal government.
	New Automated Biometric Identification System Improves Capability to Identify Terrorists Clarksburg, WV February 17, 2009 (press release BTF w/ PM Biometrics)
DoD Biometrics Process	See: Analyze, Collect, Decide/Act, Manage, Match, Reference, Share, Store.
	Derived From: Body of Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) 31 January 2008

D

DoD Electronic Biometric Transmission Specification (DoD EBTS)	The DoD EBTS is a transmission specification to be used between DoD systems that capture biometric data and repositories of biometric data. The DoD EBTS does not attempt to specify all data used in all biometric enabled applications. It does allow for the definition of application specific data elements and transactions. Department of Defense Electronic Biometric Transmission Specification 27 March 2009, Version 2.0, DIN: DOD_BTF_TS_EBTS_ Mar09_02.00.00
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. See Also: Enrollment. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

E

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. See Also: FBI Electronic Biometric Transmission Specification National Science & Technology Council (NSTC), 14 September 2006 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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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. See Also: Duplicate Enrollment Check, Full Enrollment, Re-enrollment, Tactical Enrollment. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Entire Joint Image (EJI)	An exemplar image containing all four full-finger views for a single finger: one rolled; left, center, and right plain . Derived From: ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136

E

Equal Error Rate (EER)	A statistic used to show biometric performance, typically when operating in the verification task. The EER is the location on a ROC or DET curve where the false accept rate and false reject rate (or one minus the verification rate {1-VR}) are equal. In general, the lower the equal error rate value, the higher the accuracy of the biometric system. Note, however, that most operational systems are not set to operate at the "equal error rate" so the measure's true usefulness is limited to comparing biometric system performance. The EER is sometimes referred to as the "Crossover Error Rate." See Also: Detention Error Trade-off Curve (DTE), False Reject Rate (FRR), Detection and Identification Rate, False Non-Match Rate (FNMR), Identification Rate, and Verification Rate
	Report of the Defense Science Board Task Force on Defense Biometrics. March 2007 http://www.acq.osd.mil/dsb/reports/ADA465930.pdf
Exemplar	The known prints of an individual, recorded electronically, photographically, by ink, or by another medium. See Also: Fingerprint.
	Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Glossary v2.0, May 08 2009 http://www.swgfast.org/documents/glossary/090508_Glossary_2.0.pdf

F

Face Recognition	A biometric modality that uses an image of the visible physical structure of a biometric subject's face for recognition purposes. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Failure to Enroll (FTE)	Failure of a biometric system to form a proper enrollment reference for an end user. Common failures include end users 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 and Technology Council (NSTC), 27 July 2006 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
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 2006 http://www.biometrics.gov/Documents/glossary.pdf

F

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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
False Match Rate (FMR)	Proportion of the completed biometric non-match comparison trials that result in a false match. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
False Non-Match Rate (FNMR)	Proportion of the completed biometric match comparison trials that result in a false non-match. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

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
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 2006 http://www.biometrics.gov/Documents/glossary.pdf
FBI Electronic Biometric Transmission Specification (FBI EBTS)	The FBI EBTS specifies the file and record content, format, and data codes necessary for the exchange of fingerprint, palmprint, facial, and iris information between federal, state, and local users and the FBI. It provides a description of all requests and responses associated with electronic fingerprint and other identification services. ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (EBTS) version 8.1, November 19, 2008, IAFIS-DOC-01078-8.1 https://www.fbibiospecs.org/biospecs.html
FBI Universal Latent Workstation (ULW)	The Universal Latent Workstation (ULW) is the first in a new generation of interoperable latent workstations. Several state and local agencies, the FBI, NIST, and the AFIS vendors have been working together on standards to improve interoperability and sharing of latent identification services. The ULW is part of that program. It helps agencies and AFIS vendors understand and develop the concept of encode once and search anywhere. FBI Website http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_services

F

Features	Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference. National Science & Technology Council (NSTC), 14 September 2006 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. See Also: Arch, Bifurcation, Core Point, Delta Point, Exemplar, Friction Ridge, Loop, Minutia(e), Minutia(e) Point, Platen, Ridge Ending, Slap Fingerprint, Ten Print Match, Valley, Whorl. Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/recording-legible-fingerprints/takingfps
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. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 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. See Also: Fingerprint Vendor Technology Evaluation, Flat Fingerprint, Latent Fingerprint, Plain Fingerprint, Platen, Rolled Fingerprint, Slap Fingerprint, Ten Print Match. Derived From: The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf

F

Fingerprint Vendor Technology Evaluation (2003) - (SUNSET) (FPVTE)	An independently administered technology evaluation of commercial fingerprint matching algorithms. See Also: Fingerprint Scanning. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Flat Fingerprint	Fingerprints taken in which the finger is pressed down on a flat surface but not rolled. Also known as Plain Fingerprint. See Also: Fingerprint Scanning. Derived From: Latent Fingerprint Matching: Fusion of Rolled and Plain Fingerprints, ICB, June, 2009. http://biometrics.cse.msu.edu/
Forensic	Relates to the use of science or technology in the investigation and establishment of facts or evidence. Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
Forensics	The application of multi-disciplinary science capabilities to establish facts. Capstone Concept of Operations for DoD Forensics, 4 June 2008
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. See Also: Fingerprint. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

F

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. See Also: Enrollment. Biometrics in Support of Identity Management ICD 20 June 2008

G

Gait	A biometric subject's manner of walking. This behavioral characteristic is in the research and development stage of automation. See Also: Modality.
	Derived From: National Science & Technology Council (NSTC), 14 September 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf

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 2006 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. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Hand Scan	Print from the outer side of the palm. See Also: Modality. Biometrics in Support of Identity Management ICD 20 June 2008

I

IDENT	The Automated Biometric Identification System (IDENT) is a Department of Homeland Security (DHS)-wide system for the storage and processing of biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.
	Derived From: Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) July 31, 2006
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 2006 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

I

Identity	Identity is a set of characteristics by which an entity (e.g., human, application, device, service or process) is recognizable from every other entity.
	DoD Identity Management Strategic Plan January 2009
Identity Assurance	Identity Assurance is the capability to affix, verify, and/or determine the identity of a person (living, deceased, unconscious, non-functioning, uncooperative, or unaware), an organization, or entity. It is used to protect or control access to property, people, or information or used in any situation in which the identity of an individual or a population of individuals must be known and tracked, such as non-combat relief operations, disbursement, or access to benefits.
	Biometrics Support to Identity Management JCD (31 January 2008)
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 SC37 standards bodies, Aug 2006.
Identity Dominance	Identity Dominance is defined as the operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity and/or to counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of an individual and to establish a knowledge base for that identity. This includes denying an adversary the ability to identify our protected assets.
	Derived From: Biometrics Support to Identity Management JCD (31 January 2008)

I

Identity Facilitation	Identity Facilitation is defined as 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. Identity Facilitation is conducting and supporting the business of Identity Assurance and Identity Protection through technology development and insertion, data management and storage, and information flow and facilitation.
	Body of Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) 31 January 2008
Identity 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 Intelligence	Information produced by the discovery, management, and protection of Identity attributes in support of U.S. national and homeland security interests.
	DA G2
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: NSTC Identity Management Task Force Report 2008 http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf

I

Identity Protection	Protection of identity data, safeguarding identity or specific attributes and data elements associated with a person, organization or entity from information warfare, theft, unauthorized access or unintended use.
	Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
Identity Superiority	The management, protection and dominance of identity information for friendly, neutral or unknown, and adversary personnel through the application of military operations and business functions.
	Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006
Individual	As used in the Biometrics Enterprise, an individual refers to a single human being.
	Derived From: JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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 2006 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-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
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 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Iris Exchange (IREX)	IREX (Iris Exchange) is an umbrella program for various NIST activities supporting interoperable iris biometrics. As of late 2009, three activities have been completed or are underway. The first, IREX I, addressed standards, formats and compression for data interchange. The second, IREX II, is intended to define and measure image quality. The third, IREX III, will give guidelines to users.
	National Institute of Standards and Technology / IREX Webpage http://iris.nist.gov/irex/

I

Iris Recognition	A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 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. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 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. See Also: Fingerprint Scanning.
	Derived From: National Science & Technology Council (NSTC), 14 September 2006 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 v2.0, May 08 2009 http://www.swgfast.org/documents/glossary/090508_Glossary_2.0.pdf
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). See Also: Live Scan
	Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

L

Live Scan	Optical image capture of a biometric sample in a live format instead of using ink and paper. Derived From: ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136
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 2006 http://www.biometrics.gov/Documents/glossary.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
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

L

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. See Also: Fingerprint.
	National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

M

Manage	The capability and/or process to perform administrative duties related to biometrics, such as tracking transaction status and transaction logging. See Also: DoD Biometrics Process. Body of Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) 31 January 2008
Match	Comparison decision that the recognition biometric sample(s) and the biometric reference are from the same source. Derived From: JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Match Capability	The capability and/or process to compare biometric data in order to link previously obtained biometrics and related contextual data to a particular identity for identification or verification of identity. See Also: DoD Biometrics Process. Body of Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) 31 January 2008
Mimic	The presentation of a biometric sample in an attempt to fraudulently impersonate someone other than the biometric subject. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

M

Minutia Exchange (MINEX)	MINEX is a series of NIST coordinated development efforts aimed at improving the performance and interoperability of core implementations of the INCITS 378 and ISO/IEC 19794-2 fingerprint minutia standards. MINEX 04 is designed to evaluate whether various populations and combinations of encoding schemes, probe templates, gallery templates, and fingerprint matchers will produce successful matches. MINEX II is the part of the MINEX program dedicated to the evaluation and development of the capabilities of fingerprint minutia matchers running on ISO/IEC 7816 smart cards. National Institute of Standards and Technology / MINEX Webpage http://www.nist.gov/itl/iad/ig/minex.cfm
Minutia(e)	Friction ridge characteristics which occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, bifurcation, or a more complicated "composite" type. See Also: Fingerprint. Derived From: ISO/IEC 19794-2 Information Technology - Biometric data interchange formats - Part 2: Finger minutiae data
Minutia(e) Point	The point where a friction ridge begins, terminates, or splits into two or more ridges. See Also: Fingerprint. ANSI/NIST-ITL 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
Mitochondrial DNA (mtDNA)	The DNA found in the mitochondria of the cell and inherited only from the mother. As maternal relatives will share the same mtDNA, unique identifications are not possible using only mtDNA analyses. See Also: Nuclear DNA Federal Bureau of Investigation (FBI) website, CODIS Combined DNA Index System http://www.fbi.gov/about-us/lab/codis/codis_brochure

M

Modality	A type or class of biometric sample originating from a biometric subject. For example: face recognition, fingerprint recognition, iris recognition, DNA, etc. See Also: Face Recognition, Fingerprint Recognition, Hand Geometry Recognition, Iris Recognition, Palm Print Recognition, Speaker Recognition, DNA Matching, Gait, Hand Scan, Keystroke Dynamics, Signature Dynamics.
	Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) Glossary, 4 April 2008
Mugshot	A photograph of an individual's face. Term used interchangeably with facial image. The term facial image usually implies a higher quality image than a mugshot.
	Derived From: ANSI/NIST-ITL 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
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 DNA Index System (NDIS)	One component of CODIS and the national and highest level index containing the DNA records contributed from participating federal, state and local laboratories.
	Federal Bureau of Investigation (FBI) website, Quality Assurance Standards for DNA Databasing Laboratories http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet
National Information Exchange Model (NIEM)	The National Information Exchange Model is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.
	National Information Exchange Model (NIEM) website http://www.niem.gov/index.php
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 (NIST) http://www.nist.gov/public_affairs/general_information.cfm
Non-match	Comparison decision that the recognition biometric sample(s) and the biometric reference are not from the same source.
	JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0

N

Normalized	Biometric sample or other data that has been assessed for quality considerations and adjusted to standards matching before submission and storing. See Also: Biometric Sample Derived From: AV-2 ToBe 2015 DoD Biometrics Enterprise Architecture: ICOMs
Nuclear DNA (nDNA)	The DNA contained within the nucleus of a cell. Traditional DNA testing examines numerous areas, or loci, of nDNA that differ between individuals. With the exception of identical twins, no two people have the same genetic sequence at these loci, allowing for automated biometric identification based on each person's unique nDNA profile. State of the Art Biometrics Excellence Roadmap Technology Assessment: Volume 3 DNA, March 2009

O

One-to-Many	Comparing one biometric reference to many biometric references to identify a biometric subject. Sometimes referred to as 1: n. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
One-to-One	Comparing one biometric reference to another biometric reference to identify a biometric subject. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Overt Collection	Collection of biometrics with the individual's knowledge. An example of an overt collection is a fingerprint live scan. See Also: Covert Collection Derived From: Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms

P

Palm Print	An exemplar or latent friction ridge image from the palm (side and underside) of the hand. Data Format for the Interchange of Extended Friction Ridge Features 10 May 2010
Palm Print Recognition	A biometric modality that uses the physical structure of a biometric subject's palm print for recognition purposes. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
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 (POI)	An individual for whom information needs or discovery objectives exist. Office of the Director of National Intelligence (ODNI)
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

P

Personally Identifiable Information (PII)	Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).
	DoDD 5400.11 and DoD 5400.11-R, May 8 2007 http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf
Plain Fingerprint	Fingerprints taken in which the finger is pressed down on a flat surface but not rolled. Also known as Flat Fingerprint. See Also: Fingerprint Scanning.
	Derived From: Latent Fingerprint Matching: Fusion of Rolled and Plain Fingerprints, ICB, June, 2009. http://biometrics.cse.msu.edu/
Plantar	Having to do with the friction ridge skin on the feet (soles and toes).
	Data Format for the Interchange of Extended Friction Ridge Features 10 May 2010
Platen	The surface on which the fingers, toes, palms, or soles of the feet are placed during optical image capture. Platens are also used by other types of electronic fingerprint devices (i.e. capacitive, optical, electro-optical, etc.). See Also: Fingerprint Scanning.
	Derived From: International Association for Biometrics (iAfB)

P

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 2006

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 2006 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 2006 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-enrollment requires new captured biometric sample(s). See Also: Enrollment. JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009 http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-3068_SD_2_Version_11_January_2009.pdf?nodeid=7950678&vernum=0
Reference	The capability and/or process of querying various repositories of associated information on individuals (Intelligence, Medical, Human Resources, Financial, Security, Education, Law Enforcement, etc) for analysis purposes. See Also: DoD Biometrics Process. Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

R

Response Time (SUNSET)	The time used by a biometric system to return a decision on identification or verification of a biometric sample. International Association for Biometrics (iAfB)
Ridge Ending	A minutiae point at the ending of a friction ridge. See Also: Fingerprint. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Ridge Flow	The direction of one or more friction ridges. Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Glossary v2.0, May 08 2009 http://www.swgfast.org/documents/glossary/090508_Glossary_2.0.pdf
Rolled Fingerprint	An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor. See Also: Fingerprint Scanning. National Science & Technology Council (NSTC), 14 September 2006 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 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Share	The capability and/or process to transfer (send and/or receive) biometric sample(s), contextual data, and/or associated information within the DoD and between DoD and other national, international, and non-governmental organizations (NGOs) as appropriate. See Also: DoD Biometrics Process. Derived From: Biometrics Support to Identity Management JCD (31 January 2008)
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. See Also: Modality. Derived From: National Science & Technology Council (NSTC), 14 September 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf

S

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. See Also: Fingerprint Scanning. National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Soft Biometrics	Soft biometric traits are characteristics that provide some identifying information about an individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals. Examples of soft biometrics traits include a person's height, weight, gender, eye color,ethnicity, mitochondrial DNA, and SMT. SCARS, MARKS AND TATTOOS (SMT): SOFT BIOMETRIC FOR SUSPECT AND VICTIM IDENTIFICATION; Jung-Eun Lee, Anil K. Jain and Rong Jin; Biometrics Symposium 2008 http://www.cse.msu.edu/biometrics/Publications/SoftBiometrics/LeeJainJin_SMT_BSYM2008.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. See Also: Modality.
	Derived From: National Science & Technology Council (NSTC), 14 September 2006 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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Spoofing	The ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the data base.
	National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Store	The capability and/or process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric sample(s) and contextual data on biometric subjects when and where required. See Also: DoD Biometrics Process.
	Capstone Concept of Operations for DoD Biometrics in Support of Identity Superiority, November 2006

S

Submission	The process whereby a subject provides a biometric sample to a biometric system.
	National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

T

Tactical Collection Device (TCD)	A portable system used to capture data that represent biometric characteristics of an individual. The system provides the capability to collect, store, match, share, and manage biometric information and enable a decide/act capability. BIOMETRICS TACTICAL COLLECTION DEVICE (TCD) AND BIOMETRICS ENTERPRISE CAPABILITY (BEC) ANALYSES OF ALTERNATIVES (AoAs) April 2010
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. See Also: Enrollment. Biometrics in Support of Identity Management ICD 20 June 2008
Ten (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. See Also: Fingerprint Scanning. Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil

T

Terrorist Watchlist Person Data Exchange Standard (TWPDES)	A data exchange format for terrorist watchlist data that supports the Department of State, Department of Justice, Intelligence Community under the Director of Central Intelligence, and the Department of Homeland Security to develop and maintain, to the extent permissible by law, the most thorough, accurate, and current information possible about individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism. Intelligence Community Terrorist Watchlist Person Data Exchange Standard Data Element Dictionary, IC Metadata Working Group (IC MWG) Version 2.0, 4 July 2005, UNCLASSIFIED
Tethered Biometric System	Use of biometric sensors between deployed personnel within a robust command and control architecture. Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil
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 2006 http://www.biometrics.gov/Documents/glossary.pdf
Transaction	A command, message, or an input record that explicitly or implicitly calls for a processing action. Information contained in a transaction shall be applicable to a single subject. ANSI/NIST-ITL 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

T

True Accept Rate (TAR)	A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) accepts a true claim of identity. For Example, Frank claims to be Frank and the system accepts the claim. See Also: True Reject Rate Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
True Reject Rate (TRR)	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. See Also: True Accept Rate Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Type I Error	An error that occurs in a statistical test when a true claim is (incorrectly) rejected. For example, John Claims to be John but the system incorrectly denies his claim . See Also: False Rejection Rate National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf
Type II Error	An error that occurs in a statistical test when a false claim is (incorrectly) not rejected. For example, Frank Claims to be John but the system verifies the claim . See Also: True Reject Rate National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

U

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 2006 http://www.biometrics.gov/Documents/glossary.pdf
United States Army Criminal Investigation Laboratory (USACIL)	USACIL provides forensic laboratory services to DoD investigative agencies and other federal law enforcement agencies. U.S. Army Criminal Investigation Laboratory website http://www.cid.army.mil/usacil.html
Unqualified	Sample or other data that has not been assessed for quality considerations and adjusted to standards matching before submission and storing. See Also: Biometric Sample, Normalized AV-2 ToBe 2015 DoD Biometrics Enterprise Architecture: ICOMs
Untethered Biometric System	Collection, analysis and use of biometric sensors between deployed personnel outside of a robust command and control architecture. Biometrics Identity Management Agency (BIMA) http://www.biometrics.dod.mil

V

Validation	The process of comparing biographic, contextual and sample data to pre-existing data quality thresholds as appropriate. Derived From: AV-2 ToBe 2015 DoD Biometrics Enterprise Architecture: Services
Valley	The area surrounding a friction ridge that does not make contact with an incident surface under normal touch; the area between two friction ridges. See Also: Fingerprint. Derived From: ANSI INCITS 378-2004 Information technology - Finger Minutiae Format for Data Interchange
Vascular Pattern Recognition	Automated recognition technology where the skin of the back of the hand or the finger is penetrated by near-infrared rays generated from a bank of light emitting diodes (LEDs). The reflected rays produce an image on the sensor which reveals the vascular pattern. Derived From: National Science and Technology Council (NSTC), 27 July 2006 http://www.biometrics.gov/Documents/glossary.pdf
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 2006 http://www.biometrics.gov/Documents/glossary.pdf

W

Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification (IAFIS-IC-0010 [V3]) (WSQ)	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
Whorl	A friction ridge pattern in which the ridges of the fingers, toes, palms, and soles of the feet are circular or nearly circular. The pattern will contain 2 or more deltas. See Also: Fingerprint. Derived From: National Science & Technology Council (NSTC), 14 September 2006 http://www.biometrics.gov/Documents/glossary.pdf

Acronyms

ABIS	Automated Biometric Identification System
AFDIL	Armed Forces DNA Identification Laboratory
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
AV-2	All View 2
BAP	Biometric Analysis Packet
BAT	Biometric Automated Toolset
BC	Biometric Consortium
BDT	Biometrics Data Team
BEC	Biometrics Enabling Capability
BEI	Biometric-Enabled Intelligence
BEWL	Biometrically-enabled Watchlist
BFC	Biometric Fusion Center
BG	Biometrics Glossary
BI2R	Biometric Identity Intelligence Resource
BIAR	Biometric Intelligence Analysis Report
BIMA	Biometrics Identity Management Agency
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	Biometrics 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
CLDM	Core Logical Data Model
CMC	Cumulative Match Characteristic
CMR	Cumulative Match Rate
COCOM	Combatant Command
CODIS	Combined DNA Index System

Acronyms

CONOPS	Concept of Operations
DBEKS	DoD Biometric Expert Knowledgebase System
DBIDS	Defense Biometric Identification System
DET	Detection Error Tradeoff
DHS	Department of Homeland Security
DMDC	Defense Manpower Data Center
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DoD ABIS	Department of Defense Automated Biometric Identification System
DoD EBTS	Department of Defense Electronic Biometric Transmission Specification
DoDD	Department of Defense Directive
DPI	Dots Per Inch
DRS	Detainee Reporting System
EER	Equal Error Rate
EFTS	Electronic Fingerprint Transmission Specification
EJI	Entire Joint Image
EMIO	Expanded Maritime Interdiction Operation
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FBI EBTS	Federal Bureau of Investigation Electronic Biometric Transmission Specification
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
iAfB	International Association for Biometrics
IAFIS	Integrated Automated Fingerprint Identification System
IC MWG	Intelligence Community Metadata Working Group
ICSA	International Computer Security Association
IDD	Integrated Data Dictionary
IDENT	Automated Biometric Identification System - Department of Homeland Security

Acronyms

INCITS	International Committee for Information Technology Standards
IREX	Iris Exchange
ISO	International Organization for Standardization
JCD	Joint Capabilities Document
JPEG	Joint Photographic Experts Group
JTC1/SC37	Joint Technical Committee 1, Subcommittee 37, Biometrics
LEP	Locally Employed Personnel
MINEX	Minutia Exchange
mtDNA	Mitochondrial DNA
NDIS	National DNA Index System
nDNA	Nuclear DNA
NGI	Next Generation Identification
NGIC	National Ground Intelligence Center
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTC	National Science and Technology Council
ODNI	Office of the Director of National Intelligence
ORCON	Dissemination & Extraction of Information Controlled by Originator
PDES	Person Data Exchange Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
POI	Person 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
TAR	True Accept Rate
TCD	Tactical Collection Device
TRR	True Reject Rate
TWPDES	Terrorist Watchlist Person Data Exchange Standard
ULW	Universal Latent Workstation
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
USACIL	United States Army Criminal Investigation Laboratory
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language

References

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

2 ANSI/NIST-ITL 1-2007, Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo Information

3 ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information

4 Armed Forces DNA Identification Laboratory website

5 AV-2 ToBe 2015 DoD Biometrics Enterprise Architecture: ICOMs

6 AV-2 ToBe 2015 DoD Biometrics Enterprise Architecture: Services

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

8 Biometrics Identity Management Agency (BIMA)

9 Biometrics in Support of Identity Management ICD 20 June 2008

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

11 Biometrics Support to Identity Management JCD (31 January 2008)

12 BIOMETRICS TACTICAL COLLECTION DEVICE (TCD) AND BIOMETRICS ENTERPRISE CAPABILITY (BEC) ANALYSES OF ALTERNATIVES (AoAs) April 2010

13 Body of Biometrics in Support of Identity Management, Joint Capabilities Document (JCD) 31 January 2008

14 Capability Production Document For Biometric Enterprise Core Capabilities (BECC), Version 2.0, 14 January 2008 and DoD Biometrics Overarching Integrated Product Team (OIPT) Report, April 8, 2010

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

16 Capstone Concept of Operations for DoD Forensics, 4 June 2008

17 Chemical Science and Technology Laboratory/NIST website, Quality Assurance Standards for DNA Testing Laboratories

18 Common Biometric Exchange Formats Framework (CBEFF), ANSI INCITS 398-2008

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

20 DA G2

21 Data Format for the Interchange of Extended Friction Ridge Features 10 May 2010

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

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

24 Department of Defense Electronic Biometric Transmission Specification 27 March 2009, Version 2.0, DIN: DOD_BTF_TS_EBTS_ Mar09_02.00.00

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

26 DoD Directive 8521.01E Enclosure 2

27 DoD Identity Management Strategic Plan January 2009

28 DoDD 5400.11 and DoD 5400.11-R, May 8 2007

29 ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (EBTS) version 8.1, November 19, 2008, IAFIS-DOC-01078-8.1

30 FBI Website

31 Federal Bureau of Investigation (FBI) website, CODIS Combined DNA Index System

32 Federal Bureau of Investigation (FBI) website, National DNA Index System

33 Federal Bureau of Investigation (FBI) website, Quality Assurance Standards for DNA Databasing Laboratories

References

34 Federal Bureau of Investigation (FBI) website, Taking Legible Fingerprints

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

36 Handbook No. 11-25. Commanders Guide to Biometrics in Afghanistan. April 2011

37 Initial Capabilities Document for Biometrics Enabled Intelligence (BEI). Version 1.0 26 February 2010

38 Intelligence Community Terrorist Watchlist Person Data Exchange Standard Data Element Dictionary, IC Metadata Working Group (IC MWG) Version 2.0, 4 July 2005, UNCLASSIFIED

39 International Association for Biometrics (iAfB)

40 ISO/IEC 19794-2 Information Technology - Biometric data interchange formats - Part 2: Finger minutiae data

41 Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms

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

43 JTC001-SC37-n-3068 Text of Standing Document 2(SD2) Version 11, Harmonized Biometric Vocabulary, February 28, 2009

44 Latent Fingerprint Matching: Fusion of Rolled and Plain Fingerprints, ICB, June, 2009.

45 Microbiology Procedure website

46 National Information Assurance Partnership, US Government Biometric Verification Mode Protection Profile for Medium Robustness Environments v1.0, 15 November 2003

47 National Information Exchange Model (NIEM) website

48 National Institute of Standards and Technology (NIST)

49 National Institute of Standards and Technology / IREX Webpage

50 National Institute of Standards and Technology / MINEX Webpage

51 National Science & Technology Council (NSTC), 14 September 2006

52 National Science and Technology Council (NSTC), 27 July 2006

53 National Science and Technology Council (NSTC): Biometric Standards

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

55 New Automated Biometric Identification System Improves Capability to Identify Terrorists Clarksburg, WV February 17, 2009 (press release BTF w/ PM Biometrics)

56 NSTC Identity Management Task Force Report 2008

57 NSTC Sub committee on Biometrics IAW INCITS/M1 and ISO/IEC JIYC 2 SC37 standards bodies, Aug 2006.

58 Office of the Director of National Intelligence (ODNI)

59 Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) July 31, 2006

60 Report of the Defense Science Board Task Force on Defense Biometrics. March 2007

61 SCARS, MARKS AND TATTOOS (SMT): SOFT BIOMETRIC FOR SUSPECT AND VICTIM IDENTIFICATION; Jung-Eun Lee, Anil K. Jain and Rong Jin; Biometrics Symposium 2008

62 Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) Glossary v2.0, May 08 2009

63 State of the Art Biometrics Excellence Roadmap Technology Assessment: Volume 3 DNA, March 2009

64 TC 2-22.82 Biometrics-Enabled Intelligence March 2011

65 The DOD Biometrically-enabled Watchlist (BEWL), A Revised Federated Approach, August 2009

66 The Intel Corporation website, Biometric User Authentication: Fingerprint Sensor Product Guidelines

67 U.S. Army Criminal Investigation Laboratory website

References

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

69 USCENTCOM Biometric Identification System for Access (BISA) CONOPS