ARMY, MARINE CORPS, NAVY, AIR FORCE, COAST GUARD

BIOMETRICS

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR TACTICAL EMPLOYMENT OF BIOMETRICS IN SUPPORT OF OPERATIONS

ATP 2-22.85
MCRP 3-33.1J
NTTP 3-07.16
AFTTP 3-2.85
CGTTP 3-93.6

May 2016

This publication supersedes ATP 2-22.85/MCRP 3-33.1J/ NTTP 3-07.16/AFTTP 3-2.85/CGTTP 3-93.6, dated 1 April 2014.

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

FOREWORD

This multi-Service tactics, techniques, and procedures (MTTP) publication is a project of the Air Land Sea Application (ALSA) Center in accordance with the memorandum of agreement between the Headquarters of the Army, Marine Corps, Navy, and Air Force doctrine commanders directing ALSA to develop MTTP publications to meet the immediate needs of the warfighter.

This MTTP publication has been prepared by ALSA under our direction for implementation by our respective commands and for use by other commands as appropriate.

WILLARD M. BURLESON III
Brigadier General, US Army
Director
Mission Command Center of Excellence

R. B. TURNER JR
Brigadier General (Sel), US Marine Corps
Director
Capabilities Development Directorate

S. A. STEARNEY
Rear Admiral, US Navy
Commander
Navy Warfare Development Command

TIMOTHY J. LEAHY
Major General, US Air Force
Commander
Curtis E. LeMay Center for Doctrine Development and Education

DAVID G. THROOP
Rear Admiral, US Coast Guard
Commander
Force Readiness Command

This publication is available through the following websites:
ALSA (http://www.alsa.mil/);
US Army (https://armypubs.us.army.mil/doctrine/index.html);
US Marine Corps (https://www.doctrine.usmc.mil);
US Navy at Navy Doctrine Library System (https://ndls.nwdc.navy.mil);
US Air Force at Air Force E-Publishing System (http://www.e-publishing.af.mil/);
US Coast Guard (https://cg.portal.uscg.mil/communities/hp/HPCenter/TTP/Default.aspxand);
Joint Electronic Library Plus (https://jdeis.js.mil/jdeis/index.jsp?pindex=0).

PREFACE

1. Purpose

This publication provides fundamental tactics, techniques, and procedures (TTP) for planning, integrating, and employing biometrics capabilities at the tactical level in support of operations. It provides TTP for collecting facial images, fingerprints, iris scans, deoxyribonucleic acid (DNA), palm prints, biographic, and contextual data. Adherence to procedures in this publication will improve the efficiency and effectiveness of biometric screening and collection denying enemy anonymity and reducing the risk to friendly forces.

2. Scope

This publication provides a standardized multi-Service framework for planning, integrating, and employing biometrics capabilities. It provides leaders, staffs, and operators a fundamental understanding of the impact accurate and valid data has on the overall biometrics process. Also, it provides considerations for enrollment site selection and procedures designed to maximize data quality. This publication:

a. Supplements established doctrine and TTP.

b. Describes the impact of properly collecting biometrics on operations.

c. Provides a detailed explanation of procedures.

d. Provides information to effectively organize, plan, and execute biometrics capabilities in a multi-Service environment.

3. Applicability

This multi-Service tactics, techniques, and procedures publication applies to all commanders, staffs, and operators using biometric capabilities in a permissive environment. This publication is unclassified with public release and unlimited distribution, in accordance with Department of Defense directive 5230.24, Distribution Statements on Technical Documents.

4. Implementation Plan

Participating Service command offices of primary responsibility will review this publication; validate the information; and, where appropriate, reference and incorporate it in Service manuals, regulations, and curricula as follows:

Army. Upon approval and authentication, the TTP contained herein will be incorporated into the United States (US) Army Doctrine and Training Literature Program as directed by the Commander, US Army Training and Doctrine Command (TRADOC). Distribution is in accordance with applicable directives listed on the authentication page.

Marine Corps.[1] The Marine Corps will incorporate the procedures in this publication in US Marine Corps doctrine publications as directed by the Deputy Commandant, Combat Development and Integration (DC, CD&I). Distribution is in accordance with the Marine Corps Publication Distribution System.

---

[1] Marine Corps PCN: 144 000211 00

Navy. The Navy will incorporate these procedures in US Navy training and doctrine publications as directed by the Commander, Navy Warfare Development Command (NWDC) [N5]. Distribution is in accordance with *MILSTRIP/MILSTRAP Desk Guide*, Naval Supply Systems Command Publication 409.

Air Force. The Air Force will incorporate the procedures in this publication in accordance with applicable governing directives. Distribution is in accordance with Air Force Instruction 33-360, *Publications and Forms Management*.

Coast Guard. The US Coast Guard (USCG) will incorporate the procedures in this publication as directed by the Commander, Force Readiness Command. Distribution is in accordance with the Coast Guard Directives System. The Coast Guard will utilize the procedures in this publication when operating under the tactical control of Department of Defense. At all other times, the Coast Guard will conduct biometrics in accordance with US Coast Guard standard operating procedures, but will use to this publication for a reference on best practices.

5. User Information

a. US Army Combined Arms Center; HQMC, DC, CD&I; NWDC; Curtis E. LeMay Center for Doctrine Development and Education (LeMay Center); USCG Force Readiness Command; and Air Land Sea Application (ALSA) Center developed this publication with the joint participation of the approving Service commands. ALSA will review and update this publication as necessary.

b. This publication reflects current joint and Service doctrine, command and control organizations, facilities, personnel, responsibilities, and procedures. Changes in Service protocol, appropriately reflected in joint and Service publications, will be incorporated in revisions to this document.

c. We encourage recommended changes for improving this publication. Key your comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendations directly to:

Army

Commander, US Army Combined Arms Center
ATTN: ATZL-MCD
Fort Leavenworth KS 66027-6900
DSN 552-4885 COMM (913) 684-4885
E-mail: usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil

Marine Corps

Deputy Commandant for Combat Development and Integration
ATTN: C116
3300 Russell Road, Suite 204
Quantico VA 22134-5021
DSN 278-3616/6233 COMM (703) 784-3616/6233
E-mail: doctrine@usmc.mil

Navy

Commander, Navy Warfare Development Command
ATTN: N52
1528 Piersey St, Building O-27
Norfolk VA 23511-2723
DSN 341-4185 COMM (757) 341-4185
E-mail: alsapubs@nwdc.navy.mil

Air Force

Commander, Curtis E. LeMay Center for Doctrine Development and Education
ATTN: DDJ
401 Chennault Circle
Maxwell AFB AL 36112-6428
DSN 493-7864/1681 COMM (334) 953-7864/1681
E-mail: LeMayCtr.DDJ.wrkflw@us.af.mil

Coast Guard

Commander, Force Readiness US Coast Guard
300 East Main Street Suite 1100
Norfolk, VA 23510
Comm: (757) 628-4149
E-mail: HQS-SG-M-FORCECOM-TTP-All@uscg.mil

ALSA

Director, ALSA Center
114 Andrews Street
Joint Base Langley-Eustis VA 23665-2785
DSN 575-0902 COMM (757) 225-0902
E-mail: alsadirector@us.af.mil

This page intentionally left blank.

SUMMARY OF CHANGES

ATP 2-22.85/MCRP 3-33.1J/NTTP 3-07.16/AFTTP 3-2.85/CGTTP 3-93.6, *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations*.

This revision:

Updates:

- Language used in chapter I and establishes definitions of common biometrics terms.
- Information by consolidating chapters II and III and appendices C and D into chapter II.
- The biometrics collection checklist with a new version.
- Chapter IV, Biometrics Collection; it is now chapter III.
- Appendix B, Department of Defense-Approved Collection Devices; it is now appendix A.
- Appendix E, Biometrics Collection Checklist; it is now appendix C.

Adds:

- Chapter II, Biometrics in Operations.
- Appendix B, Biometrics Planning Checklist.

Deletes:

- All material addressing the HIIDE as an approved Department of Defense biometric system.
- Chapter II, Tactical Roles and Responsibilities.

This page intentionally left blank.

***ATP 2-22.85**
MCRP 3-33.1J
NTTP 3-07.16
AFTTP 3-2.85
CGTTP 3-93.6

ATP 2-22.85	**US Army Training and Doctrine Command** **Joint Base Langley-Eustis, Virginia** **US Army Combined Arms Center** **Fort Leavenworth, Kansas**
MCRP 3-33.1J	**Headquarters, USMC, Deputy Commandant, CD&I** **Quantico, Virginia**
NTTP 3-07.16	**Navy Warfare Development Command** **Norfolk, Virginia**
AFTTP 3-2.85	**Curtis E. LeMay Center for Doctrine Development and Education** **Maxwell Air Force Base, Alabama**
CGTTP 3-93.6	**Force Readiness US Coast Guard** **Norfolk, Virginia**

6 MAY 2016

BIOMETRICS

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR TACTICAL EMPLOYMENT OF BIOMETRICS IN SUPPORT OF OPERATIONS

*Supersedes ATP 2-22.85/MCRP 3-33.1J/NTTP 3-07.16/AFTTP 3-2.85/CGTTP 3-93.6, dated 1 April 2014.

List of Figures

EXECUTIVE SUMMARY

BIOMETRICS

Multi-Service Tactics, Techniques, and Procedures (MTTP) for Tactical Employment of Biometrics in Support of Operations establishes tactics, techniques, and procedures for planning, integrating, and employing biometric capabilities and improving the efficiency and effectiveness of biometric screening and collection.

Chapter I Overview of Biometrics

Chapter I describes the biometrics process, defines key biometric terms, and familiarizes users with biometrics databases.

Chapter II Biometrics in Operations

Chapter II provides training, planning (by function), and employment considerations at the tactical level. It also describes the Department of Defense (DOD) Biometric Enabled Watchlist.

Chapter III Biometrics Collection

Chapter III describes the procedures to collect biometrics specific modalities electronically and using alternate methods.

Appendix A Department of Defense Approved Collection Devices

Appendix A describes the current biometric devices used by DOD.

Appendix B Biometrics Planning Checklist

Appendix B provides a checklist for tactical-level planners to incorporate biometric capabilities into operations.

Appendix C Biometrics Collection Checklist

Appendix C provides a checklist for biometric device operators.

PROGRAM PARTICIPANTS

The following commands and agencies participated in creating this publication:

Joint

Joint Exploitation Training Center, Fort Bragg, North Carolina

Army

US Army Combined Arms Center, Fort Leavenworth, Kansas
US Army Central Command, MacDill Air Force Base, Florida
US Army Training and Doctrine Command (TRADOC), Joint Base Langley-Eustis, Virginia
Intelligence Center of Excellence, New Systems Training and Integration Division, Fort Huachuca, Arizona

Marine Corps

Deputy Commandant, Combat Development and Integration, Capabilities Development Directorate, Quantico, Virginia
Command and Control Center for Excellence, Quantico, Virginia
Marine Corps Tactics and Operations Group, Twentynine Palms, California

Navy

Navy Warfare Development Command, Norfolk, Virginia
Chief of Naval Operations, OPNAV96C4, Washington, DC

Air Force

Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, Alabama
US Air Force Central Command, Shaw Air Force Base, South Carolina

Coast Guard

Force Readiness Command, US Coast Guard, Norfolk, Virginia
Headquarters, Maritime Law Enforcement, Washington, DC

Other

Defense Forensics and Biometrics Agency, Washington, DC
Global Operations Section, CJIS Division, Federal Bureau of Investigations, West Virginia

Chapter I
OVERVIEW OF BIOMETRICS

1. General

Biometrics are the measurable physical and behavioral characteristics that can establish and verify an individual's identity. These characteristics allow commanders to determine individuals who may pose a threat and segregate them from those who do not pose a threat. Integrating biometrics capabilities enables commanders to focus on joint and combined operations by helping to identify adversaries, allies, and neutral persons while degrading threat networks. Operators currently collect facial images, fingerprints, iris images, deoxyribonucleic acid (DNA) samples, palm prints, voice samples and associated contextual data (i.e., elements of biographic data and situational information) from individuals encountered during operations.

2. Definitions

It is imperative that commonly accepted biometric terms and definitions are used to ensure clarity and common understanding among the Services. The following are basic biometrics terms and definitions taken from the Defense Forensics and Biometrics Agency's Common Biometrics Vocabulary version 1 dated 30 April 2013 and Army Tactical Publication 2-22.82 dated 2 November 2015. (See the glossary for more terms and definitions.)

a. Authoritative Source. The primary Department of Defense (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 sharing 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.

b. Biographic Data. Data that describes physical and non-physical attributes of a biometric subject from whom biometric sample data has been collected. These include full name, age, height; weight, address, telephone number; email address, birthplace; nationality; education level, and group affiliations. Also, data covers employer, security clearances, and financial and credit history.

c. Biometric Data. Computer data about an individual created by biometric systems during an enrollment, verification, or identification process.

d. Biometric File. The standardized individual data set resulting from one or more biometric enrollments. The biometric file is composed of the biological, biographical, and behavioral characteristics and contextual data.

e. Biometric Identification. The automated process of comparing a submitted biometric sample against all biometric files (one-to-many) to determine whether it matches any of the templates and, if so, return the identity of the individual whose file was matched.

f. Collect. The capability and/or process to capture biometric sample(s) and related contextual data from a scene and/or a biometric subject, with or without his or her knowledge.

g. 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.

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

Note: A standard enrollment consists of a ten-print slap, two iris images, and facial image capture. Some enrollments, depending upon the mission, may be hasty in nature. In these cases, enrollments must include at least two fingerprints (indexes), two iris images, and required text fields (See chapter III for the required text fields).

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

j. Verification. The one-to-one process of matching a biometric subject's biometric sample against his/her stored biometric file.

3. The Biometric Process

The DOD biometric process relies on five biometric actions (i.e., collect, normalize, match, store, and share) and three analytical/operational actions (i.e., analyze, provide, and decide/act) that, together, provide specific outputs to support operations. Two of these actions, collect and decide/act, require operator inputs to accomplish them; while the other processes are automated. By combining these actions, the result is a much higher degree of certainty when identifying an individual or verifying a person's identity. Figure 1 depicts the DOD biometric process.

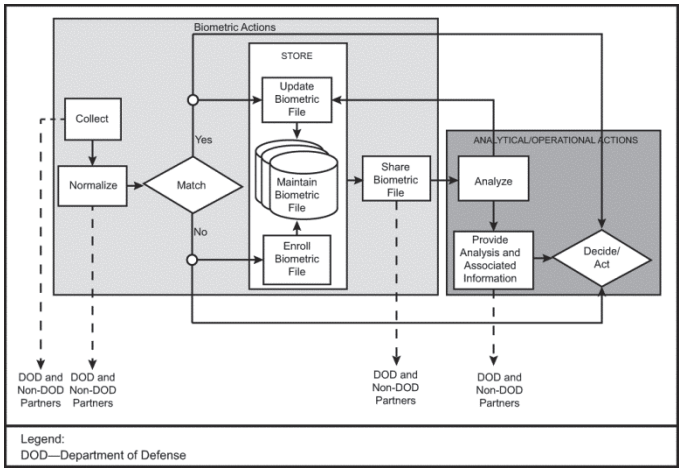

Figure 1. The Biometric Process

a. Collect. Collect is the capability or process to capture biometric samples and related contextual data from a scene or subject, with or without his/her knowledge. The collection begins with an operator who captures biometric samples (i.e., facial image, fingerprint, palm print, iris image, voice print, or DNA sample) and related contextual data from an individual, with a tactical collection device. Collection can occur at the point of an encounter or as the result of sharing from non-DOD partners. The objective is to collect standardized, high-quality biometric samples with the required biometric data. The collection must be simple enough that any operator can complete it with minimal training and equipment. Once the operator collects a biometric sample and contextual information, and places them in a file, the file is transmitted to the authoritative biometric database for matching. The authoritative biometric database which receives the biometric file will acknowledge receipt of the transmitted information and notify the operator. (See chapter III for more information on biometric modality collection techniques.)

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

(a) Facial images are collected using a camera and specialized software.

(b) Facial images are large files requiring a large amount of storage space and high bandwidth to transmit them in a timely manner.

(c) Facial recognition is not relied upon as a modality for matching at the tactical level, but may prove useful when other biometric and contextual data is available.

(2) Fingerprint Recognition. A biometric (and forensic) modality that uses the physical structure of a biometric subject's fingerprint for recognition purposes.

(a) Most often, operators use specialized, live-scan hardware and software to collect fingerprint images digitally. Fingerprint images also can be collected manually (i.e., ink and a 10-print fingerprint card).

(b) Collecting the highest quality fingerprint image is critical and minutiae points are the most important features used in fingerprint recognition.

(c) Rolled fingerprint images are preferred because they capture more fingerprint surface and minutiae points, allowing for a greater chance of a match being made against a previously collected and stored latent or live fingerprint.

(d) Individual fingerprint images are relatively small files requiring less storage space and medium bandwidth to transmit in a timely manner.

(e) Fingerprint recognition is not relied upon as a modality for matching at the tactical level, but may prove useful when other biometric and contextual data is available.

(3) Iris Recognition. A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes.

(a) Iris images are relatively small files requiring little storage space and low bandwidth to transmit in a timely manner.

(b) Iris recognition is the primary modality for matching in a tactical environment.

(4) DNA Matching. A process used to identify individuals by characteristics of their DNA. Also, DNA matching is referred to as DNA profiling, DNA testing, or DNA typing.

(a) DNA samples consist of collected DNA molecules found in bodily fluids (e.g., sweat, blood, and saliva), which are quantified, amplified, separated, and analyzed.

(b) DNA samples are generally collected and shipped to an authorized laboratory for analysis, as DNA collection often requires specialized equipment.

(c) Although DNA matching is very accurate, it is not used as a modality for matching at the tactical level.

(5) Palm Print Recognition. A biometric (and forensic) modality that uses the physical structure of a biometric subject's palm prints for recognition purposes.

(a) Palm print images are collected through a manual process (i.e., ink and palm print card) and assist in latent sample matching. Many latent samples are not fingerprints, but prints from the sides of the hand or palms due to holding an item or building a particular device.

(b) Palm print images are large files requiring a large amount of storage space and high bandwidth to transmit in a timely manner.

(c) Palm print recognition is not relied upon as a modality for matching at the tactical level, but may prove useful when other biometric and contextual data is available.

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

(a) Voice samples are digitized recordings of an individual's speech patterns and inflections.

(b) Voice sample files are large, requiring a large amount of storage space and high bandwidth to transmit in a timely manner.

(c) Voice sample collection requires specialized equipment and, generally, is collected in a controlled environment normally not available in the tactical environment.

(d) Voice recognition is not used as a modality for matching at the tactical level.

b. Normalize. The process of transforming biometric files so they are in a standard format and meet a specified level of quality. This ensures biometric files can be used by DOD and other automated biometric systems.

(1) Generally, biometric systems can create normalized biometric files at the point of collection. Typically, normalization of a biometric file is an automated action of the DOD biometrics process requiring little to no human intervention.

(2) Biometric data is automatically converted to a standardized biometric file used to match, store, or share with other DOD and non-DOD partners.

c. Match. The match action begins with receipt of the collected standardized biometric file. Matching is the capability and/or process to compare biometric data to link previously obtained biometrics and related contextual data to a particular identity for identification or verification. Matching consists of either a one-to-one (verification) or one-to-many (identification) search. Upon receipt of a positive match, the operator may receive prompt feedback providing additional information on an individual to assist with the decide/act action.

(1) Verification. In the case of a one-to-one match to verify an individual's claimed identity, the result will be in the form of a "yes" or "no" decision

associated with an underlying level of confidence. A “no” means the collected sample cannot be matched to any of the stored samples within the biometric files. A “yes” means the sample matches one or more stored biometric samples on a particular individual. Typically, a verification decision is provided by the collection device. The “yes” or “no” decision will be provided to the user who initiated the collection and transmitted it for verification.

(2) Identification. An operator or analyst located at the authoritative source can make an identification. In the case of a one-to-many identification match, the collection device will provide a “no match”, “match”, or “multiple match” response. With a “multiple match” response, the final decision is left up to the operator on the ground, the operator’s immediate supervisor, the tactical commander, or otherwise detailed by the unit’s standard operating procedures (SOPs).

(3) Completed Process. Once the matching process is complete, the collected biometric sample and contextual data will be enrolled into a repository as a new biometric file or as an update to an existing file. The enroll subaction occurs every time a one-to-many match result is negative, except where restricted by law or policy. The update subaction occurs every time an “identification” or “verification” match result is positive, except where limited by law or policy.

d. Store. Store is the capability and/or process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric samples and contextual data on biometric subjects. All enrollments are stored on a collection device and need to be transmitted to the authoritative source, per local SOP, where they are maintained and updated for future use. There are three types of biometric storage; authoritative, local trusted, and local untrusted:

(1) Authoritative Source. There are three primary United States (US) Government approved repositories for biometric information: DOD’s Automated Biometric Identification System (ABIS), Department of Homeland Security’s (DHS’s) IDENT and the Department of Justice’s (DOJ’s) Next Generation Identification (NGI). Although the DOD primarily uses ABIS, all three repositories screen biometric information. There must be a communication path to access any of the repositories. All biometric files will be enrolled within the appropriate authoritative source at the earliest possible opportunity, except where limited by law, policy, or directive.

(2) Local Trusted Source. A local trusted source is a subset of the authoritative source and is established to accomplish a specific function within an operational mission. Reasons for establishing a local trusted source might include insufficient network connectivity to provide immediate access to the authoritative source or an operational need for closed-loop access. If a match is not made against a local trusted source, the file should be queried against the authoritative source for a match.

(3) Local Un-trusted Source. A local un-trusted source is a local repository of biometric files which 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 sharing biometric information. Because of the potential unreliability of their information, local untrusted sources should be used only when absolutely necessary.

e. Share. Share is the capability and/or process to transfer (send and/or receive) biometric sample(s), contextual data, match result and/or associated information within the DOD and between DOD and other national, international, and nongovernmental organizations (NGOs) as appropriate and in accordance with applicable laws, policies, authorities and agreements. For the purposes of this publication, authorized sharing of biometric files is applied as follows:

(1) Among DOD-approved sources to ensure consistency across the enterprise.

(2) Among the DOD, interagency, and multinational partners as appropriate.

(3) Between the DOD and non-DOD partners, as appropriate.

f. Analyze. Analysis converts data to actionable information and recommendations, as applicable, to increase situational awareness and better understand possible courses of action. It integrates information obtained from biometric enrollments and operational processes. Analysis leverages both sources of data to support the decision making process. During analysis, an individual's biometric file is linked to associated information to reveal patterns and determine disposition. Simply knowing an individual's enrollment matches another enrollment may be of minimal value. Analysis includes determining where the individual previously came in contact with friendly forces and any additional open-source information or intelligence about the individual.

g. Provide. Provide is 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. ("Provide" is commonly referred to as reference.)

h. Decide/Act. Decide/act prompts action based on a biometric file's match results and analysis of associated information. The operator initially determines what to do with the individual at the enrollment site. The analytical response enables the forward commander to make an informed decision regarding what action to take, if any, against the individual identified. The decision to release, detain, or grant access to an individual is a key element of force protection and counterinsurgency operations. The objective is to use biometrics to enable informed decision-making when it is combined with other sources of information.

4. Databases

DOD maintains several key information systems which organize and store collected, processed, exploited, and analyzed information and materials to support identity activities and analyses. The two main systems are ABIS and biometric identity intelligence resource (BI2R).

a. DOD ABIS. ABIS is the primary authoritative database for biometric information collected on non-DOD personnel throughout the course of operations. ABIS contains fingerprints, iris images, facial images, and palm prints collected through direct enrollments; site exploitation activities; direct multinational submissions; and information shared by interagency and foreign partners. This data is stored in an unclassified repository for comparison against future biometric collections. In addition to the DOD data sources, there are multiple authoritative databases available to support DOD biometric screening activities. ABIS can share biometric files and associated information with other authoritative interagency databases (e.g., DOJ's NGI and DHS's IDENT).

b. BI2R. BI2R is an automated database that stores biometric and associated intelligence data from DOD collection devices. Analysts use the BI2R toolset to conduct analyses and develop intelligence reports supporting DOD and national missions. The system is designed to provide the DOD, intelligence community, 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. BI2R is the primary mechanism used to develop and maintain the DOD biometrically-enabled watchlist (BEWL). Biometric intelligence analysis reports (BIARs) are created and stored on BI2R. BIARs represent available biometric and all source data fused into an analyzed package available for analysts and warfighters to access via BI2R.

Chapter II
BIOMETRICS IN OPERATIONS

1. Introduction

Leaders play an integral part in implementing biometric capabilities by ensuring they are leveraged across the conflict continuum. Units and organizations must understand how biometric data may be used globally, across all components of the US Government, and with international partners. Leaders must also ensure biometric supported operations are not treated as “check-the-block” activities, but as tools to safeguard national security interests. Planning, integrating, and employing biometrics at the tactical level are accomplished in a deliberate manner, which requires tactical staffs to consider how and when to employ these capabilities.

2. Commander and Staff Tasks

The following leader and staff task considerations are presented as methods for a staff to integrate biometric capabilities into operations. Depending on the unit and type of operation being conducted, responsibility and assignment of tasks will be determined by the unit commander.

Note: As a best practice, participate in applicable biometric working groups to synchronize operations.

a. Commander.

(1) Provides direction on the intent and the requirement to integrate biometric capabilities into applicable operations.

(2) Makes biometric collection a key task and part of the commander’s Intent.

(3) Issues guidance to the staff for inclusion of biometrics capabilities during course of action development.

(4) Complies with all laws or established policies on the collection, sharing, and using biometrics.

(5) Exercises realistic expectation management for results from biometric enrollments (i.e., the results from collection and analysis take time).

b. Intelligence Section.

(1) Advises commanders on intelligence requirements related to biometrics.

(2) Provides guidance on using biometrics for counter intelligence, force protection and screening, and human intelligence operations.

(3) Ensures collected biometric enrollments are transferred to the appropriate database on a daily basis.

(4) Leverages BI2R for biometrically-baselined identity data to develop intelligence products.

(5) Monitors reported hits from the BEWL and ensure watchlist notifications and updates are disseminated to higher headquarters and subordinate units.

(6) Synchronizes additions, modifications, and deletions of watchlist identities with the authoritative DOD BEWL.

(7) Ensures biometric capabilities are included as part of the unit's collection plan.

c. Operations Section.

(1) Develops and coordinates unit policies and procedures (e.g., SOPs) to guide biometrics-enabled force protection measures.

(2) Ensures biometric collection tasks are included as part of all planned operations.

(3) Ensures disseminated DOD BEWL and local watchlists are uploaded into tactical collection devices by units, according to the unit's SOPs. Ideally, the BEWL should be updated on devices daily, but may be updated weekly as the minimum standard.

(4) Incorporates biometrics tasks into training (see Paragraph 5, Incorporating Biometrics into Training).

(5) Coordinates training to support leader, staff, and individual biometric training requirements.

d. Logistics Section.

(1) Advises the commander on resourcing requirements with regards to biometrics equipment.

(2) Ensures required consumable items are ordered or on hand to support subordinate units' biometric collection efforts.

(3) Ensures maintenance support for tactical collection devices is established.

(4) Ensures the maintenance status for tactical collection devices is reported in staff estimates.

(5) Is responsible for equipment accountability, serviceability, and replacement.

e. Communications Section.

(1) Establishes and maintains a communication architecture (e.g., portable satellite communications capabilities, Nonsecure Internet Protocol Router Network, SECRET Internet Protocol Router Network, Combined Enterprise Regional Information Exchange System (CENTRIXS), etc.) for the tactical collection devices.

(2) Incorporates biometrics collection devices into mission analysis and the primary, alternate, contingency, and emergency communications plan.

(3) Plans for degraded operations and data transfer in austere environments.

f. Legal Section.

(1) Advises the commander of the legal considerations when using biometrics.

(2) Reviews criteria for nominations to the BEWL and the associated planned actions for encounters to ensure compliance with applicable laws.

Note: An example of a legal constraint is the recent addition of biometric capability use in counter-drug operations in the Western hemisphere. The use of biometric data is restricted to a narrow scope of non-US persons aboard vessels interdicted in international waters that are treated without nationality and suspected of, or engaged in, illicit activities (see *Biometrics-at-Sea: Business Rules for South Florida* for more information.)

g. Installation/Base/Forward Operating Base Commander.

(1) Establishes and executes an installation access control program supported with biometrics and BEWL capabilities.

(2) Establishes the adjudication authority for access.

3. DOD BEWL

a. The DOD BEWL is a categorical listing of persons of interest that were vetted through a nomination process managed by the DOD BEWL manager (Army/National Ground Intelligence Center). The categorical listing provides contextual data for decision making when encountering and biometrically identifying an individual on the watchlist. These categories are grouped in the following focus areas. Individuals may have multiple categories associated with them:

(1) Criminal.

(2) Force protection.

(3) Forensics.

(4) Joint task force (JTF) or command specific.

(5) Mission area specific.

(6) National directives.

(7) Organizational persons of interest.

(8) Wanted.

b. The focus area most commonly seen by the collector on the ground is JTF or command specific, a subset list of categories from the DOD BEWL. This JTF BEWL provides clear directives for actions taken when encountering and biometrically identifying individuals. During the enrollment or identification process, the collection device provides notification to the operator that the individual is on the BEWL and directs an action. The primary actions are detain, question, deny access or privileges, or track movement.

c. JTF commanders will determine criteria for applying the action-based categories, taking into account applicable rules of engagement and host nation laws.

(1) At a minimum, nominations to all categories must have a biometric sample (i.e., fingerprints, iris images, or facial image).

(2) Nomination of US persons must meet retention requirements found in Executive Order 12333, *United States Intelligence Activities*, as amended.

d. Nominations to the DOD BEWL must meet the following minimum criteria for the specific categories to which the individual is nominated:

(1) Probability of threat (i.e., placement, capability, motivation, etc.)

(2) Known or suspected intent (e.g., comments, derogatory reporting, etc.)

(3) Circumstantial factors (e.g., associations, criminal activity, misconduct, etc.)

(4) Suspicious activity.

(5) Medical reasons.

e. Upon encountering an individual, instructions for actions are provided by the information uploaded in the collection device.

4. Networks, Connectivity, and Data Transmission

For biometric collection screening and enrollment to be successful, the biometric data must move from the point of collection to an authoritative source for processing, comparison, and storage (see Figure 2, Biometrics Data Flow). The method of data movement will depend on mission and availability of communications. The following are the two primary means of data transmission.

a. Web-Based Portal. The DOD has various web-based portals for transferring biometric data and information to appropriate entities for processing, comparison, and analysis. These portals are available on unclassified and classified networks; and in some instances, the North Atlantic Treaty Organization's Battlefield Information Collection and Exploitation System. When required, the portals can be accessed through an operation-specific network (e.g., CENTRIXS). The portals are broadly accessible through multiple communication links, including local area networks (LANs) and Broadband Global Area Networks. However, bandwidth issues can be significant, limiting factors, especially in non- and semi-permissive and austere environments. Planners should ensure the unit communications officer, granted the authority to operate one or both of these portals on the theater-based network, and the appropriate Service-level agreements are in place for each of the authoritative repository management organizations.

b. Dedicated Server Architecture. A few primary collection systems within the DOD operate entirely off their system-specific infrastructure of servers (i.e., Biometrics Automated Toolset). These servers operate in a distributed fashion from a central hub; ensuring stored data is continuously synchronized. The central hub provides the connection to DOD's authoritative biometrics repositories which, in turn, manage automated information exchanges with interagency repositories. These systems can provide robust support in confined theaters with a well-developed communications network, however, they can require significant manpower to maintain and service.

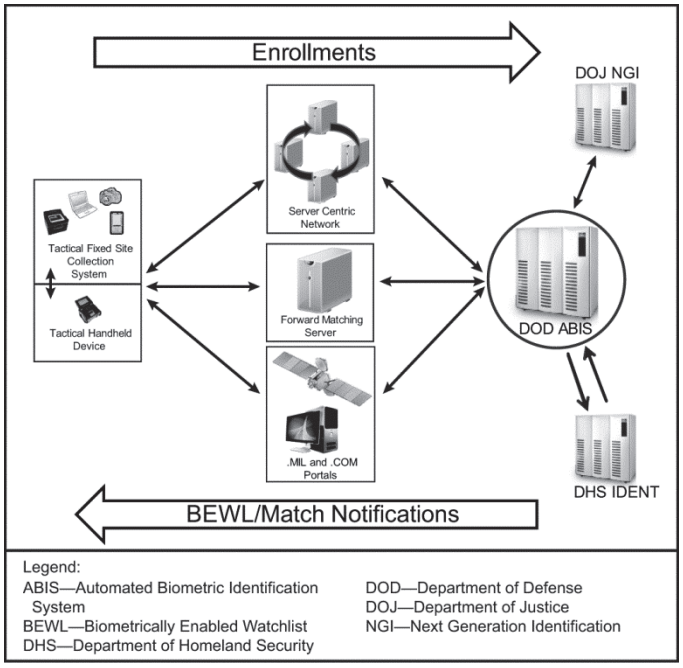

Figure 2. Biometric Data Flow

5. Planning and Integrating Biometrics Capabilities in Operations

a. Mission Types.

(1) The specific mission types described in this chapter are NOT all inclusive as some missions may fall under multiple operational categories.

(2) Depending on the mission, employing biometrics capabilities can enhance the commander's effectiveness in conducting operations. The five following operational categories provide biometrics integration aspects that staff members should consider as they conduct their planning.

(a) Combat Operations.

- Checkpoint or Cordon and Search. Enables identification of individuals and enrollment of unknown individuals.
- Targeted or Raid. Provides identity confirmation of known targets, associates, and casualties.

(b) Support Operations.

- Counter-narcotics. Identifies persons involved in manufacturing, transporting, and distributing narcotics.

- Counter-piracy. Identifies parties involved in piracy and tracks their movement.
- Detainee Operations. Provides identity verification and tracking throughout the detainee management process.
- Census Operations. Provides general population enrollment in combat zones or areas of interest to populate databases.

(c) Humanitarian Assistance.

- Manage Humanitarian Aid. Ensures the right individuals receive the right aid and do not "double dip".
- Population Management. Identifies and monitors local population movement.
- Non-combatant Evacuation Operations. Identifies, tracks, and relocates evacuees.
- Medical Operations. Identifies patients to properly account for resources, ensure they receive appropriate treatment, and families are reunited after a disaster.

(d) Border Control.

- Undocumented Individuals Interdiction. Biometrics enrollment allows identification and tracking of unknown or wanted persons.
- Entry Control. Verifies the identity of individuals crossing borders.
- Maritime Alien Migrant Interdiction Operations. Collects biometrics at sea to process individuals and make prosecution or repatriation decisions.

(e) Force Protection.

- Base Access. Identifies persons who desire access to a given facility, base, or port; turns away those who have been denied access, and detains persons who are linked to a criminal or terrorist incident.
- Personnel Vetting. Screens employed persons and local nationals providing contract services (which aids in the vetting process), enhances operational area security, and denies access to undesirable personnel; and limits the flow of funds to insurgent and terrorist groups.

(f) Personnel Recovery Operations. This includes authenticating isolated personnel during personnel recovery operations. These include the following examples:

- Biometric information of isolated personnel and perpetrators of the isolating event.
- Latent samples.

- Computer messages.
- Messages left behind.
- Behavioral analysis of the last known location of the isolated personnel (i.e., soil samples, tool marks, or casts of impressions).

b. Biometrics Employment Considerations.

(1) Biometrics collection by tactical units may be subject to legal parameters, international agreements, or other arrangements between the US and other countries. Command guidance will direct the appropriate implementation of these capabilities, which must be clearly articulated to subordinate units to ensure operations are conducted according to legal guidelines.

(2) Remember, proper site selection for biometrics enrollment during dynamic operations can impact the mission. Time, personnel, and communication requirements must be considered to ensure proper execution and commitment of resources.

(3) Select a location that supports the flow of personnel, type of operation, security risks; biometrics tasks, expected number of operators and enrollees, user circumstances; existing data, and type and amount of equipment.

(4) Select a location that reduces the environmental impacts of dust, sunlight, and other factors that can limit or prevent the successful biometrics collection because they may interfere with the equipment's ability to accurately record data.

(5) Work closely with local leaders in the area of operations and gain acceptance and support of biometrics enrollment operations. If possible, ensure a trained female operator is available to facilitate working with female enrollees.

(6) Refer to Chapter III, Biometric Collection, and appendices for additional information.

6. Incorporating Biometrics into Training

Units should conduct training according to Service-specific requirements, ensuring all members of the command understands their roles and responsibilities in the biometrics process. The following are training considerations.

a. Leader Training. Doctrine and tactics training for leaders and key personnel include:

(1) Biometrics capabilities as force multipliers and the impact on operations and force protection.

(2) Specific tasks that maximize the use of biometric capabilities to enhance missions.

(3) Biometrics capabilities and incorporating their use during assessments, planning, and operations.

(4) Infrastructure requirements (e.g., communications, facilities, etc.) and logistical support.

(5) Principles to understand the DOD BEWL categories and nomination procedures.

b. Individual Training. Most operations provide the opportunity to collect biometrics. When operators are trained on biometrics collection equipment, they become faster and more efficient. This equates to a high quality, and quantity, of enrollments. Tasks for initial and sustainment training include:

(1) Preparing the collection device for operation.

(2) Collecting biometrics.

(3) Acting on identification and watchlist alerts.

(4) Transferring data for enrollments and watchlists.

Note: For the latest training materials, visit the milSuite Biometrics Training milWiki at https://www.milsuite.mil/wiki/Biometrics_Training. (A Common Access Card is required.)

c. Collective Training. Integrate biometrics capabilities into collective training events that include role players and provide opportunities for collections, identifications, verifications, and enrollments.

Chapter III
BIOMETRICS COLLECTION

1. Modalities

Note: Operators can collect biometric data from deceased personnel to verify their identity. This may present certain challenges based on what equipment sets are available and the condition of the remains.

a. Facial Images.

This is the first of four primary biometric modalities collected in support of operations. The following is required to ensure facial images are properly collected:

(1) Use a clean and neutral background without additional personnel, maps, equipment, vehicles, vessels, etc.

(2) Do not allow the person to wear glasses or any other items obscuring the area being photographed. The person may choose to expose only the area from ear to ear and hairline to chin (i.e., they do not have to remove a headdress). There are no constraints on cosmetics.

(3) Include the subject's image from the top of the head to the bottom of the neck, including the ears (e.g., passport or identification card sized photos). See figure 3 for proper alignment and orientation of facial images. Criminal enrollment requires photos that include front; right and left profiles; and right and left 45-degree, angled images.

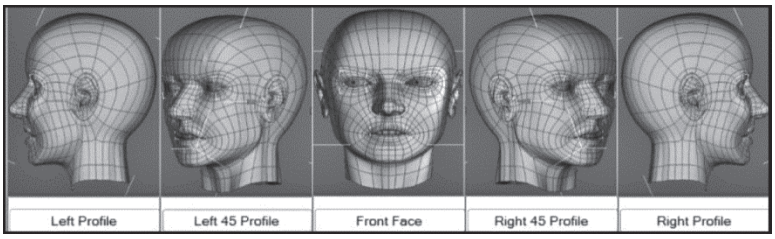

Figure 3. Proper Alignment and Orientation of Facial Images

(4) Ensure the subject's face is free of shadows and is not in direct light. Improper lighting will create shadows, and direct light will create a shine on the subject's face.

(5) Ensure the camera is level and the subject's face is positioned straight and postured toward the camera to ensure a useful front facing photograph. Generally, have the camera lens at the subject's nose height to prevent distortion.

(6) Capture profile pictures with the subject's head facing in the direction of the body.

(7) To capture a subject's facial image during low-light conditions or at night, supplemental light sources should be placed approximately 45

degrees off the center of the subject's face and pointed at the subject's chest.

b. Electronic Fingerprint Collection. A proper fingerprint should be complete, free of smears, and show friction ridges. See figure 5 for an example of a proper rolled and slap fingerprint. The following is required to ensure proper fingerprint collection.

Note: A tactical enrollment is a DOD Flat Print Rap Sheet Search requiring a full ten print collection and contextual data.

(1) Ensure the subject's fingers and collection surface are clean prior to collection. Excessive dirt, grease, and dryness of the print area will likely result in an unreadable fingerprint capture. The following is information about the silicone platen:

(a) Clean the fingerprint capture device to remove residual fingerprint images, dirt, oils, and other debris. Use the appropriate method for the device.

(b) The silicone platen increases the intimate contact area for friction ridge image capture. The silicone surface enables easily and rapidly capturing fine, worn, and dry finger ridge detail.

(2) Maintain control of the subject's finger using slight and consistent pressure for a slap or rolled fingerprint. Look at the print on screen to ensure it is clear. See figure 4 for a method to control the subject, and figure 5 for a proper display using the Secure Electronic Enrollment Kit II (SEEK II).

Figure 4. Proper Finger Control for a Two-Finger Slap

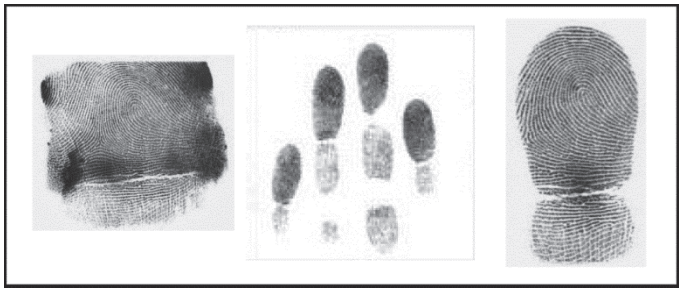

Figure 5. Rolled Print, Four Finger Slap Print, and Single Flat

(3) When collecting rolled fingerprints, roll the subject's finger from knuckle in to knuckle out and from nail in to nail out (i.e., from the subject's uncomfortable position to comfortable position). Thumbs are rolled towards the subject's body, while fingers are rolled away from subject's body. Rolled prints are always preferred and should be collected whenever possible.

c. Ink Palm Print Capture. The palm print card is a supplement to the criminal or civil fingerprint card and is not intended to stand alone from the actual fingerprint card. Palm prints should be complete, free of smears, and show friction ridges. Figures 6–9 demonstrate the proper locations to ink the palm and proper palm captures on the palm print and supplemental palm print cards.

Note: This modality is primarily collected at detention facilities. Refer to the facility's SOP for more procedures on using this method.

(1) Collect palm prints using black roller ink, an FBI Form FD 884 (Palm Print Card), and an FBI Form FD 884a (Standard Supplemental Fingerprint Finger and Palm Print Card). Each palm will require its own set of cards.

Note: Operators must be trained and proficient in collecting wet-ink fingerprinting for this to be a viable option.

(2) Ensure the subject's fingers and collection surface are clean prior to collecting palm prints. Excessive dirt, grease, or dryness of the print area may result in an unreadable print.

(3) Complete a palm print card as follows:

(a) Roll a coat of black ink along the writer's palm of the hand (also called the ulnar side, as in figure 6) from the base of the wrist to the fingertip and roll writer's palm impression within the capture block.

(b) Roll a coat of ink on the index finger and capture a print in the appropriate block. This print will match and verify the palm print with the ten print fingerprint card.

(c) Roll a coat of ink on the entire palm and fingers (from the base of wrist to the finger tips), capturing a print in the appropriate box. Ensure the captured print mirrors the palm illustration in the capture box.

(d) Complete the back of the card by rolling fingers in the same manner used on ten print cards.

(e) Repeat for the other palm.

Note: To avoid smudging, complete palm prints on both hands, on the same side of the cards prior to rolling prints on the reverse side of each card.

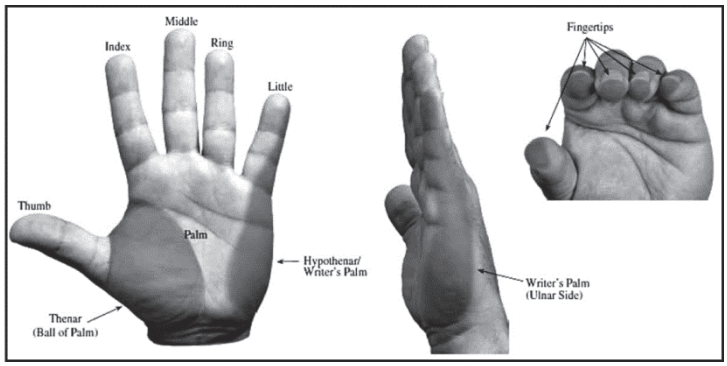

Figure 6. Ink Palm Capture Areas

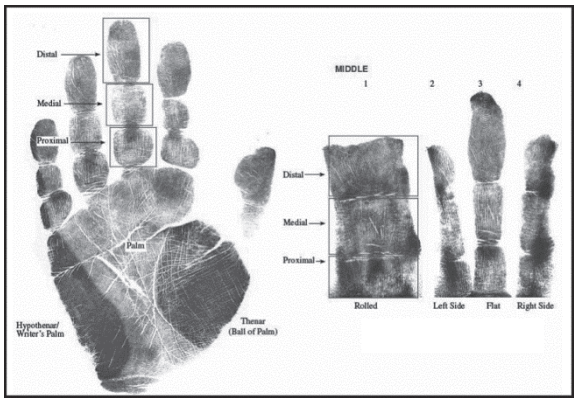

Figure 7. Hand with Basic Ink Regions

Figure 8. Ink Palm Capture

(4) Complete the supplemental finger and palm print cards as follows:

(a) Select the left or right hand and check appropriate box.

(b) Ink the appropriate portion of the palm.

(c) Capture the print oriented in the direction of the text (and hand image) within each capture block. Each impression must be captured fully within the box provided, in a vertical, upright position.

(d) Capture the impressions for each digit: fully rolled, left edge, flat, and right edge.

Note: All digits must be captured in the following sequence: fully rolled, left edge, flat, right edge, contain impressions of the distal, medial, and proximal portions of each finger.

(5) Repeat the process for opposite hand.

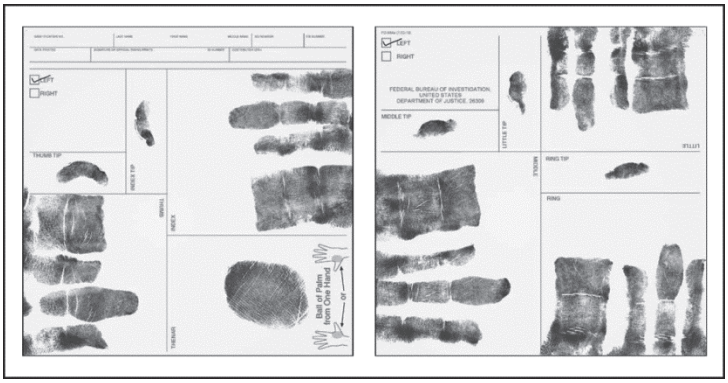

Figure 9. Ink Supplemental Finger and Palm Capture

d. Iris. The iris is the colored area of the eye. The captured image should show the iris and pupil to the maximum extent possible with no glare obscuring any part of the iris. See figure 10 for an example of a proper iris image. The following are required to ensure proper collection of an iris capture.

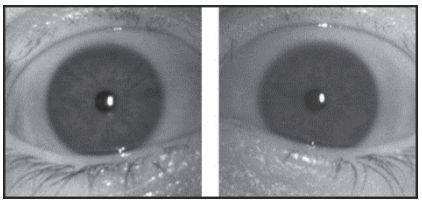

Figure 10. Proper Iris Image

(1) Remove any obstructions from the subject's iris, including glasses, contact lenses, eyelashes, hair, etc.

(2) Place the subject so you can view the display on a iris capture device and ensure the image captures at least 75% of the iris. See figure 11 for proper position for SEEK II iris captures.

Figure 11. Iris Capture with SEEK II

(3) Ensure the subject's eyelids are open, to the maximum extent possible.

(4) Have subjects open their eyes wide and remain still to avoid excessive eye movement.

(5) Avoid direct light that may place a glare over the iris.

e. Voice Sample Collection.

(1) Voice is a biometric modality based on the measurable physical characteristics of an individual's voice and can verify or refute an identity.

(2) Voice Identity Biometrics Exploitation Services(VIBES). VIBES is a means of providing tactical speaker identification and exploitation of collected voice samples. It provides web-based and mobile device applications that support the collection and submission of voice samples to the VIBES server for biometric voice matching. VIBES can provide insight into: who is communicating with whom; where individuals and groups are and have been over time; and associations among individuals and specific activities or events. VIBES can be used in cooperative, non-cooperative or stand-off modes to recognize individuals without regard for the communications channel used, the language spoken, or the truthfulness of speaker dialog to quickly identify individuals.

(3) Voice recognition can support personnel recovery, force protection, site exploitation, and civil engagement missions.

f. DNA. DNA may be obtained from an inner cheek or bodily fluids. DNA is very sensitive to contamination, which would make the samples useless. If possible, secure DNA samples in clean, sterile container immediately after collection. The collector should ensure DNA is properly collected by using the following directions.

(1) Wear latex gloves to avoid contact with the sample. Do not let samples come in contact with each other and change gloves after each individual sample.

(2) Use a sterile buccal (cheek) swab to collect a sample from the subject's inner cheek or other source for bodily fluids (e.g., blood). Use the swab on only one person. If swabbing the cheek, tear off one end of the packaging, remove the swab, and keep the packaging. Insert the swab against the inside of the individual's cheek. Move the swab up and down while gently rolling the swab against the cheek for at least 15 seconds. Collect minimal saliva. See figure 12.

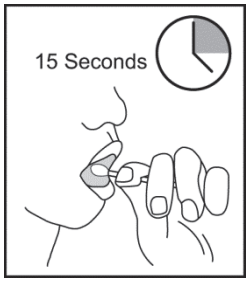

Figure 12. Cheek Swab

(3) Try to collect bodily fluids from an uncontaminated area on the subject's body.

(4) If time permits, allow the sample to dry in open air for one minute before placing it in a container. Avoid putting the sample into a plastic bag or returning the swab to a culture media tube to prevent degradation due to moisture which exacerbates mold, fungus, or bacterial growth. Instead, put the evidence into a clean paper bag, envelope, or the original paper swab packaging. Line the container with a blank sheet of paper to prevent fluids from leaking through onto other samples. Place only one individual's sample in a container to avoid cross-contamination. Use tape, not staples, to secure the container. Store DNA samples in a cool, dark, dry place until shipped. When sending DNA samples to a lab, always use paper products to ship the samples. This allows continued drying of the sample. Follow the unit's SOP for shipping DNA samples to a lab.

2. Biographic and Contextual Data

a. The collector should enter accurate and complete information.

b. Names and places should be spelled out phonetically and written in the most accepted manner or based on a transliteration guide. Adherence to a transliteration guide is crucial as it enables name searching within intelligence databases.

c. Mandatory entries for the biographic and contextual data are indicated in the following list. As the situation and guidance dictate, add the information in the optional fields based on the type of enrollment conducted.

(1) Mandatory entries:

(a) Name.

(b) Person type (e.g., enemy prisoner of war, host nation hire, etc.).

(c) Reason printed (e.g., detainee, detainee visitor, badge, etc.).

(d) Date printed.

(e) Country of birth.

(f) Date of birth.

(g) Gender.

(h) Race.

(i) Height.

(j) Weight.

(k) Hair color.

(l) Eye color.

(m) Date of arrest (only mandatory if completing a criminal enrollment).

(2) Optional Entries:

(a) Identification number (e.g., passport, national identification, detainee number, etc.).

(b) Phone number.

(c) Occupation.

(d) Place of residence.

(e) Family members' names.

(f) Marital status.

(g) Organization memberships.

(h) Other names used.

(i) Location of encounter (e.g., Global Positioning System coordinates, military grid reference system, grid location, or description of enrollment site.

3. Alternative Biometrics Collection Methods

In the event of electronic biometrics collection device failure, consider the following methods for biometrics collection.

a. Facial Image Capture.

(1) A standard digital camera can capture a high-quality facial image (i.e., greater than 3.5 megapixels).

(2) Tips for successfully taking facial recognition images include the following:

(a) Use a flash.

(b) Use a mid-range zoom setting to avoid optical distortion.

(c) Show a capture tag or name.

(d) Show ears clearly.

(e) Remove glasses.

(f) Position the camera at the subject's nose height for ALL images.

(g) Avoid causing the subject to squint; use a fill flash, if necessary.

Note: Using a personal digital camera may be prohibited in the area of operation.

b. Fingerprints.

(1) Fingerprints can be collected using a black ink pad and a ten print card (i.e., a card specifically designed for capturing inked fingerprints; a Federal Bureau of Investigation card, such as FBI Form FD 249 (Arrest and Institution Fingerprint Card); or a tactical ten print slap card). See figures 13 and 14 for an example of a wet ink capture set and a slap card, respectively. Refer to chapter III, paragraph 1.b., for fingerprint collection techniques and illustrations

Note: Operators should be trained and proficient in collecting ink fingerprints for this to be a viable option.

Figure 13. Ink Print Capture Card

Note: Only fold finger print cards along the lines to prevent smudging prints.

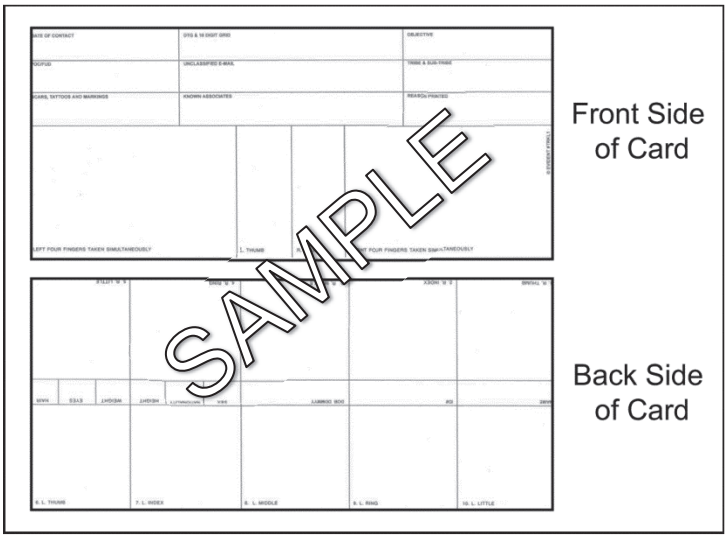

Figure 14. Tactical Ten Print Slap Card

(2) When electronic and ink methods are unavailable, a plain fingerprint impression can be obtained by performing the following steps.

(a) Record, on a white piece of paper, the name of the subject, time, and date with the grid location on either bottom corner of the paper.

(b) Fold the paper in half.

(c) Have the subjects wipe their fingers lightly across the side of their nose with both hands at least three times to pick up the oil on the skin.

(d) Have the subjects run their hands through their hair three times to pick up the oil in the hair.

(e) Hold the folded paper and have the subjects press their fingertips from both hands onto the paper, making sure to get the tips of the fingers (i.e., one-fourth inch below the first joint).

c. Iris. There is no approved alternative collection method for an iris image.

d. DNA.

(1) If sterile buccal swabs are unavailable, use a small, sterile gauze pad or sterile, commercial cotton swab to swab the inside of the mouth to capture a viable DNA sample.

(2) If using a sterile, cotton swab, either swab the individual with both ends of it or indicate on the packaging or swab which end was used to collect the sample.

(3) The collection source should be placed back in its packaging or sealed in a non-plastic container for transport. See chapter III, paragraph 1.f., for more information.

Note: There is no alternate collection for a voice sample.

e. Contextual Data

(1) If there are any biometrics collected using the alternative methods, properly link the contextual information and biometrics record.

(2) See chapter III, paragraph 2.c., for specific examples of important contextual data needed to support a complete biometrics enrollment.

This page intentionally left blank.

Appendix A
DEPARTMENT OF DEFENSE-APPROVED BIOMETRIC SYSTEMS

1. Secure Electronic Enrollment Kit II (SEEK II)

a. Function. SEEK II (pictured in figure 15) collects fingerprints, iris images, facial photos, and biographical and contextual data of persons of interest and matches fingerprints and iris images against an internal, biometrically-enabled watchlist.

b. Description. It is a lightweight, multimodal collection and matching device, compatible with the Department of Defense Automated Biometric Identification System, compliant with current software standards, and fully operational in direct sunlight.

Figure 15. SEEK II

c. Equipment Data.

(1) Dimensions: 5 inches (in) (127 millimeters (mm)) by 8 in (203 mm) by 3 in (76 mm).

(2) Weight: 4 pounds (lbs) (1.82 kilogram).

(3) Operating Temperature Range: 35 degrees Fahrenheit (F) to 120 degrees F (2 degrees Celsius (C) to 49 degrees C).

(4) Two gigabytes (GBs) of dynamic random access memory (DRAM).

(5) Sixty-four GB solid state flash drive, removable with tools.

(6) Back-lit, full QWERTY keyboard with right and left mouse buttons and touch-pad cursor control.

(7) Microphone and speaker.

(8) Two hot-swappable 7.4 volt, 2.4 Ah (ampere-hour) rechargeable Lithium ion batteries with 3 hours of operation for each battery (which have a push-button charge indicator).

(9) Wi-Fi 802.11B/G; Bluetooth; 3G (optional).

(10) Ethernet (RJ-45).

(11) Dual-iris capture.

(12) A 1.3 mega pixel (1280 X 1024) Mug Shot Camera with LED illumination, torch and flash.

(13) Fingerprint scanner with two-finger scan and rolled fingerprint collection.

2. Biometrics Automated Toolset–Army (BAT-A)

a. Function. The BAT-A (figure 16) collects fingerprints, iris scans, facial photos, and biographical information from persons of interest for entry into a searchable database.

b. Description. The BAT-A consists of a laptop computer and separate peripherals for collecting biometrics. The toolset connects to any computer server geographically distributed across an area of operations that store biometrics data. The toolset system is used to identify and track persons of interest and to document and store information about them, such as interrogation reports. It is compatible with the SEEK II device.

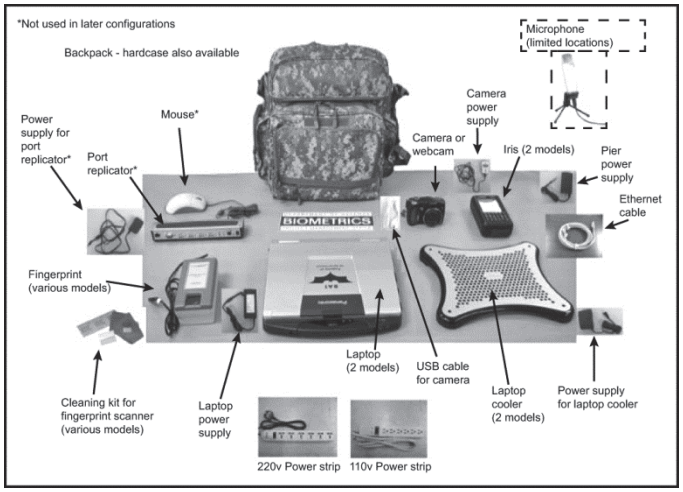

Figure 16. BAT-A

c. Equipment Data.

(1) Weight: Up to 21 lbs.

(2) Operating Temperature Range: 35 degrees F to 120 degrees F (2 degrees C to 49 degrees C).

(3) Up to 4 GB of DRAM.

(4) 500 GB hard drive.

(5) Microphone and speaker with voice capture capability.

(6) Wi-Fi 802.11B/G; Bluetooth.

(7) Ethernet (RJ-45).

(8) Dual- and single-iris capture.

(9) Three mega pixels (1280 X 1024) combination camera and iris image collection.

(10) Fingerprint scanner with four-finger slap and rolled fingerprint collection.

This page intentionally left bank

Appendix B
BIOMETRICS PLANNING CHECKLIST

- ☐ Identify the amount of equipment needed for unit or base operations.
  - o Patrol _____
  - o Traffic Control Point _____
  - o Entry Control Point _____
  - o Quick Reaction Force _____

- ☐ Unit, location, and personnel to maintain the biometrics devices (including username and password)
- ☐ Watchlist updated by whom and when
- ☐ The device is fully functional with a full battery charge and checked as part of the mission pre-brief.
- ☐ Within the Pre-brief:
  - o Verify the team has appropriate username and passwords.
  - o Verify the team can operate the device.
  - o Provide a recommendation of when to employ the device based on the task (i.e., entry control point, patrol, quick reaction force)
  - o Establish criteria for individuals you can enroll/identify.
  - o Provide examples of an incident report.
  - o Identify actions that should be taken after watchlist match notification.
- ☐ Collect the biometrics devices as a part of the debriefing process.
  - o Identify how many enrollments were completed.
  - o Identify how many incident reports were completed.
  - o Export data and transfer it to a server or portal.
  - o Charge batteries.
- ☐ Check the quality of biometric enrollments.

This page intentionally left blank.

Appendix C
BIOMETRICS COLLECTION CHECKLIST

- ☐ The tactical collection device (TCD) batteries are fully charged.
- ☐ The TCD is fully operational.
- ☐ At least two Service members are trained on the device and have access (e.g., current usernames and passwords).
- ☐ The TCD has the current biometrically-enabled watchlist (BEWL).
- ☐ Actions upon encountering a BEWL hit.
- ☐ All deceased individuals, if possible, may be identified. If there is a positive match on the BEWL or a previous enrollment appears, indicate deceased within the incident report.
- ☐ Return the TCD and notify leadership of BEWL hits and the number of enrollments.

This page intentionally left blank.

REFERENCES

ARMY

ATP 2-22.82, *Biometrics-Enabled Intelligence*, 02 November 2015

COAST GUARD

USCG Biometrics-at-Sea: Business Rules for South Florida, Version 4, March 2008. (FOUO)

USCG Maritime Law Enforcement Manual, COMDTINST M16247.1 (series).

JOINT PUBLICATIONS

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 February 2016).

JP2-0, *Joint Intelligence,* 22 October 2013

OTHER PUBLICATIONS

American National Standards Institute/National Institute of Standards and Technology ANSI/NIST-ITL 1-2000, http://www.nist.gov/itl/ansi/upload/sp500-245-a16.pdf (last accessed on 11APR2016)

DOD Biometrics Enterprise Architecture (Integrated) v2.0, Common Biometric Vocabulary CBV v1.0, Defense Forensics and Biometric Agency Programs Division, April 2013, http://www.dfba.mil/Files/Documents/References/common%20biometric%20vocabulary.pdf (last accessed on 11APR2016)

DOD Capstone Concept of Operations for Employing Biometrics in Military Operations, 10 June 2012, http://www.biometrics.dod.mil/Files/Documents/Collaborations/DOD%20Capstone%20Concept%20of%20Operations%20for%20Employing%20Biometrics%20in%20Military%20Operations%20Approved%2010%20Jun%2012.pdf (last accessed on 11APR2016)

DODD 8521.01E, *Department of Defense Biometrics*, 21 FEB 2008, http://dtic.mil/whs/directives/corres/pdf/852101p.pdf, accessed 11APR2016.

Executive Order 12333 (as amended), *United States Intelligence Activities*, 4 Dec 1981, http://www.archives.gov/federal-register/codification/executive-order/12333.html (last accessed on 11APR2016)

FBI Form FD 249 (Arrest and Institution Fingerprint Card), https://www.fbi.gov/about-us/cjis/forms/description-fd249 (last accessed on 11APR2016)

FBI Form FD 884 (Palm Print Card), https://www.fbi.gov/about-us/cjis/forms/description-fd88 (last accessed on 11APR2016)

FBI Form FD 884a (Standard Supplemental Fingerprint Finger and Palm Print Card), https://www.fbi.gov/about-us/cjis/forms/description-fd884a (last accessed on 11APR2016)

Homeland Security Presidential Directive-6, Integration and Use of Screening Information, 16 Sep 2003, https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf (last accessed on 11APR2016)

Homeland Security Presidential Directive 11, Comprehensive Terrorist-Related Screening Procedures, 27 Aug 2004, http://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-7.html (last accessed on 11APR2016)

National Ground Intelligence Center, Department of Defense Biometrically-Enabled Watchlist Categorical Glossary, Version 1.3, August 2014

National Security Presidential Directive-59/Homeland Security Presidential Directive-24, Biometrics for Identification and Screening to Enhance National Security, 5 Jun 2008, http://www.biometrics.gov/PresidentialDirectives/Default.aspx (last accessed on 11APR2016)

NATO STANAG 4715, Biometrics Data, Interchange, Watchlisting And Reporting, Edition 1, 04 October 2013, http://nso.nato.int/nso/nsdd/stanagdetails.html?idCover=8035&LA=EN (last accessed on 11APR2016)

NATO STANAG 4715 AEDP-15, Biometrics Data, Interchange, Watchlisting And Reporting, Edition A Version 1, 4 October 2013, http://nso.nato.int/nso/nsdd/APdetails.html?APNo=1495&LA=EN (last accessed on 11APR2016)

WEBSITES

“Biometrics Training”, https://www.milsuite.mil/wiki/Biometrics_Training (last accessed on 12ARP2016)

Defense Forensics & Biometric Agency, www.bometrics.dod.mil (confirmed on 12 APR 2016)

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

A

ABIS	automated biometric identification system
Ah	ampere hour
ALSA	Air Land Sea Application

B

BAT-A	Biometrics Automated Toolset - Army
BEWL	biometrically-enabled watchlist
BI2R	biometric identity intelligence resource
BIAR	biometric intelligence analysis report

C

C	Celsius
CD&I	Combat Development and Integration
CENTRIXS	Combined Enterprise Regional Information Exchange System

D, E

DHS	Department of Homeland Security
DNA	deoxyribonucleic acid
DOD	Department of Defense
DOJ	Department of Justice
DRAM	dynamic random access memory

F

F	Fahrenheit

G

GB	gigabyte

H

HQMC	Headquarters, Marine Corps

I

in	inch

J, K

JTF	joint task force

L

lb	pound
	M
mm	millimeter
MTTP	multi-Service tactics, techniques, and procedures
	N, O, P, Q, R
NATO	North Atlantic Treaty Organization
NGI	Next Generation Identification
NGO	nongovernmental organization
NWDC	Navy Warfare Development Command
	S
SEEK II	Secure Electronic Enrollment Kit II
SOP	standard operating procedure
	T
TCD	tactical collection device
TRADOC	Unites States Army Training and Doctrine Command
TTP	tactics, techniques, and procedures
	U
US	United States
USCG	United States Coast Guard
	V, W, X, Y, Z
VIBES	Voice Identity Biometrics Exploitation Services

PART II – TERMS AND DEFINITIONS

arch—A friction ridge 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. (Source: DOD Biometrics Enterprise Architecture (Integrated) v2.0, Common Biometric Vocabulary (CBV) v1.0)

automated biometric identification system—Generic term for any automated biometric identification system. Also called ABIS. (Source: CBV v1.0)

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. (Source: CBV v1.0)

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. (Source: CBV v1.0)

Biometric Automated Toolset—A multimodal biometric system that collects, stores, and shares fingerprints, iris images, and facial photography. It is used to enroll, identify, and track persons of interest, build digital dossiers on individuals that can include attached digital images, documents, and a wide variety of reports such as: biographic, contextual, relationship, and interrogation reports. BAT-A has an internal biometric signature search/match capability and can be configured into either a mobile or handheld configuration. Also called BAT-A. (Source: CBV v1.0)

biometric capture device—A device that collects a signal from a biometric characteristic and converts it to a captured biometric sample. (Source: CBV v1.0)

biometric capture process— Process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample. (Source: CBV v1.0)

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. (Source: CBV v1.0)

biometric data—Computer data about an individual created by biometric systems during an enrollment, verification, or identification process. (Source: ATP 2-22.82)

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. (Source: CBV v1.0)

biometric identification—The automated process of comparing a submitted biometric sample against all biometric files (one-to-many) to determine whether it matches any of the templates and, if so, return the identity of the individual whose file was matched. (Source: ATP 2-22.82)

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. (Source: CBV v1.0)

biometric identity intelligence resource—An automated database that stores biometric and associated intelligence data from DOD collection devices. Analysts use the BI2R toolset to conduct analyses and develop intelligence

reports supporting DOD and national missions. The system is designed to provide the DOD, intelligence community, 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. Also called BI2R. (Source: CBV v1.0)

biometric information—Provides a part of the overall intelligence picture and helps to confirm or deny identities of combatants and noncombatants in the area of operations. Biometric information is fused with other information and intelligence to develop all-source intelligence. (Source: ATP 2-22.82)

biometrics-enabled intelligence—The intelligence derived from processing biologic identity data and other all-source for information concerning persons of interest. Also called BEI. (JP 2-0)

biometrically-enabled watchlist— Any list of person of interests, with individuals identified by biometric sample instead of by name and the desired/recommended disposition instructions for each individual. (Source: CBV v1.0)

biometric sample—A biological specimen or a representation (e.g., digital, analog, etc.) of biometric characteristics prior to biometric feature extraction. (Source: CBV v1.0)

biometric subject—An individual from which biometric samples were collected. (Source: CBV v1.0)

collect—The capability and/or process to capture biometric samples and related contextual data from a biometric subject, with or without his or her knowledge. (Source: CBV v1.0)

contextual data— Elements of biographic data and situational information (who, what, when, where, how, why, etc.) associated with a collection event and permanently (Source: CBV v1.0)

Defense Forensics and Biometrics Agency—[This agency] leads, consolidates, and coordinates forensics and biometrics activities and operations for the Department of Defense in support of identity operations. (Source: http://www.biometrics.dod.mil/About/mission.aspx)

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. (Source: CBV v1.0)

DOD electronic biometric transmission specification— The DOD electronic biometric transmission specification (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. (Source: CBV v1.0)

enrollment— The process of collecting contextual data and a biometric sample from a biometric subject, converting the sample into a biometric reference, and storing the data in the biometric system's database for later comparison. (Source: CBV v1.0)

face recognition— A biometric modality that uses an image of the visible physical structure of a biometric subject's face for recognition purposes. (Source: CBV v1.0)

fingerprint— An impression of the friction ridges of all or any part of the finger. (Source: CBV v1.0)

flat fingerprint— Fingerprint taken in which the finger is pressed down on a flat surface but not rolled. Also known as Plain Fingerprint. (Source: CBV v1.0)

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. (Source: CBV v1.0)

identity intelligence— The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. Also called I2. (Source: JP 2-0)

iris recognition— A biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes. (Source: CBV v1.0)

latent fingerprint— A fingerprint "image" left on a surface that is dormant or hidden until circumstances are suitable for development or manifestation. (e.g., 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.) (Source: CBV v1.0)

latent sample— A biological residue that is dormant, inactive, or non-evident but can be captured, measured and stored. (Source: CBV v1.0)

loop—A friction ridge 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. (Source: CBV v1.0)

modality— A type or class of biometric sample originating from a biometric subject (e.g., face recognition, fingerprint recognition, iris recognition, etc.). (Source: CBV v1.0)

palm print— An impression of the friction ridges of all or any part of the palmar surface of the hand. (Source: CBV v1.0)

palm print recognition— A biometric and forensic modality that uses the physical structure of a biometric subject's palm print for recognition purposes. (Source: CBV v1.0)

person of interest—An individual for whom information needs or discovery objectives exist. (Source: CBV v1.0)

plain fingerprint— Fingerprint taken in which the finger is pressed down on a flat surface but not rolled. Also known as Flat Fingerprint. (Source: CBV v1.0)

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.). (Source: CBV v1.0)

rolled fingerprint— An image that includes fingerprint data from nail to nail, obtained by “rolling” the finger across a capture surface. (Source: CBV v1.0)

Secure Electronic Enrollment Kit II—A tactical handheld biometric collection device capable of comprehensive, multimodal identification and enrollment. It combines forensic-quality fingerprint capture, rapid dual iris image capability, and facial capture technology. The device automatically captures and formats standards-based flat and rolled fingerprints and iris and facial images. (Source: ATP 2-22.82)

slap fingerprint— Fingerprints taken by simultaneously pressing the four fingers of one hand onto a capture surface. Slaps are known as four finger simultaneous plain impressions. (Source: CBV v1.0)

ten (10) print match or identification— A positive identification of a biometric subject that is obtained by comparing each of his or her 10 fingerprints to those in a system of record. It is usually performed by an automated fingerprint identification system and verified manually by a human fingerprint examiner. (Source: CBV v1.0)

valley— A lowered portion of the epidermis on the palmar or plantar skin, consisting of those areas between ridges. (Source: CBV v1.0)

Verification—The one-to-one process of matching a biometric subject's biometric sample against his stored biometric file. Also known as Authentication. (Source: CBV v1.0)

Whorl— A friction ridge pattern in which the ridges are circular or nearly circular. The pattern will contain 2 or more deltas. (Source: CBV v1.0)

***ATP 2-22.85**
MCRP 3-33.1J
NTTP 3-07.16
AFTTP 3-2.85
CGTTP 3-93.6

6 MAY 2016

By Order of the Secretary of the Army

Official:

MARK A. MILLEY
General, United States Army
Chief of Staff

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1611102

DISTRIBUTION:
Active Army, Army National Guard, and US Army Reserve: To be distributed in electronic media only (EMO).

By Order of the Secretary of the Air Force

TIMOTHY J. LEAHY
Major General, USAF
Commander
Curtis E. LeMay Center for Doctrine Development
and Education

ACCESSIBILITY:	Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.
RELEASABILITY:	Approved for public release; distribution is unlimited. This determination was made on 07AUG2015.

* Supersedes ATP 2-22.85/MCRP 3-33.1J/NTTP 3-07.16/AFTTP 3-2.85/ CGTTP 3-93.6, dated 1 April 2014.

MARINE CORPS PCN: 144 000211 00 PIN: 103962-000