ATP 2-22.82

Biometrics-Enabled Intelligence (U)

(FEF for FOIA Request)

November 2015

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies and their contractors only as it contains critical information concerning intelligence sources and methods that is exempt from disclosure under provisions of AR 25-55, 1 November 1997, paragraph 3-200, exemption number 3, subparagraph h; and DODI C-5240.08, *Counterintelligence (CI) Security Classification Guide*, dated 28 November 2011. This determination was made on 15 September 2015. Other requests must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ 85613-7017, or via e-mail at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Requests to release of this document to foreign entities must be referred to the requestor's supporting foreign disclosure office.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document in accordance with AR 380-5.

This publication supersedes TC 2-22.82, dated 21 March 2011.

Headquarters, Department of the Army

~~FOR OFFICIAL USE ONLY~~

*ATP 2-22.82

Army Techniques Publication
No. 2-22.82

Headquarters
Department of the Army
Washington, DC, 2 November 2015

Biometrics-Enabled Intelligence (U)
(FEF for FOIA Request)

Contents (U)

---

*This publication supersedes TC 2-22.82, dated 21 March 2011.

Figures (U)

Tables (U)

Preface (U)

(U) ATP 2-22.82 provides guidance concerning the use of biometric information by intelligence professionals, protection operations personnel, personnel involved in detainee screening or operations, and personnel involved in targeting operations.

(U) ATP 2-22.82 is concerned principally with biometrics-enabled intelligence (BEI), the fundamentals of biometrics, and biometric systems, as well as with biometric tools used in current operations. ATP 2-22.82—

- Includes the biometric processes in support of the intelligence process during the full range of military operations.
- Outlines roles and responsibilities of intelligence units and individuals using biometrics in current operations.
- Discusses intelligence considerations for the use of biometrically enabled watch lists (BEWLs).

(U) ATP 2-22.82 includes examples of activities military intelligence Soldiers are likely to encounter in operations and incorporates lessons learned from various operations, including the technical and operational experiences of subject matter experts in biometrics and military intelligence.

(U) The principal audience for ATP 2-22.82 are Army intelligence professionals engaged in intelligence production. Others include commanders, staffs, and trainers at all Army echelons and national-level agencies and centers. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this manual.

(U) Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 27-10.) In addition, intelligence databases are subject to intelligence oversight and the Privacy Act of 1974 with regard to any U.S. person information they may contain. Commanders and intelligence leaders ensure their organizations comply with the provisions of EO 12333, DOD 5240.1-R, and AR 381-10 pertaining to the collection, retention, and dissemination of information on U.S. persons.

(U) ATP 2-22.82 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 2-22.82 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ATP 2-22.82 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. ATP 2-22.82 uses BEI-related terms that correspond with standardized Department of Defense (DOD) biometric terminology. These terms are italicized and their definitions are not followed by a proponent publication.

(U) ATP 2-22.82 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

(U) The proponent of ATP 2-22.82 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Capabilities Development and Integration Directorate, U.S. Army Intelligence Center of Excellence. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-CDI-D (ATP 2-22.82), 550 Cibeque Street, Fort Huachuca, Arizona 85613-7017; by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

Introduction (U)

BIOMETRICS IN RECENT OPERATIONS (U)

(U) The collecting, matching, and intelligence analysis of biometric data supports positive identification and characterization of individuals who may pose a threat to U.S. national security. It provides a powerful capability for DOD to identify and respond to threat personnel, protect friendly forces, and defend national interests. The success of DOD and DOD's partners in identifying such threats is further improved by sharing biometric data with interagency and international partners. Therefore, it is important to employ a comprehensive, coordinated approach for biometric data collection, as well as to foster sharing agreements with interagency and foreign partners.

(U) The term *biometrics* is derived from the Greek words "bio" (life) and "metrics (to measure). Automated biometric systems have become available only over the last few decades, as significant advances have been made in computer processing. However, many of these new automated techniques are based on ideas that were originally conceived hundreds, even thousands of years ago.

(U) Army units began biometric data collection from local populations in Kosovo in the Balkans during the 1990s as a way of tracking locally employed personnel. Biometric data collection continued to evolve during operations in Iraq and Afghanistan. These two theaters of operations demonstrated the difficulty in fighting an enemy who could hide among the local population.

(U) Incorporating biometric information into all-source intelligence analysis was, and continues to be, a highly successful technique for enabling U.S. forces to strip away the anonymity of threat fighters hiding among the local population. With an extraordinary degree of confidence, U.S. forces were able to link enemy activity to nonuniformed, previously unidentified combatants using biometrics technology.

(U) Despite the success of biometrics, BEI, and BEWL employment in combat zones, there remained an underlying problem—inefficiency. A contributing factor to this problem was the sheer mass of data accumulated. During operations in Iraq, the Army provided deployed forces with biometric collection devices without a comprehensive plan for how the data would be collected, managed, and employed by units. The efforts of combining the lessons learned from biometric collection and operational best practices led to more efficient targeted collection.

LESSONS FROM RECENT OPERATIONS (U)

(U) Several important lessons emerged during these operations in the last decade.

(b) (3)

(b) (3)

USE OF BIOMETRIC INFORMATION (U)

(U) Commanders require the ability to link a biometric identity to a given individual. Commanders employ biometric capabilities to deny threat forces anonymity and freedom of movement, and to positively identify known threats. These capabilities collect biometric data and combine them with contextual data to produce a biometric file on the individual. Personal identification includes positively identifying friendly, adversary, and nonadversary forces. Intelligence-related functions that biometrics and BEI can support or enhance include—

- Intelligence analysis.
- Forensic-enabled intelligence (FEI).
- Document and media exploitation (DOMEX).
- Screening of foreign national and local employee hires.
- Counterintelligence and force protection.
- Interrogation and detention operations.
- High-value target confirmation (including high-value individuals and individuals killed in action).
- Base access and local security.
- Population control or census (screening, enrolling, and badging operations).

SUMMARY OF CHANGES (U)

(U) Introductory table-1 summarizes doctrinal changes made by this manual. Introductory table-2 on page viii lists changes to terms made by this manual.

Introductory table-1. (U) Summary of changes

Chapter 1—Overview
Chapter 1 revises chapter 1 of the superseded manual. Additions include— • Modification of the Army's definition of biometrics-enabled intelligence (BEI). • Introduction of biometrics support to the Army intelligence process.
Chapter 2—Biometric Processes
Chapter 2 incorporates portions of chapters 1 and 2 of the superseded manual addressing biometric processes. The chapter discusses— • The biometric automated process and biometric automated actions. • The biometrics-enabled intelligence process. • Integration of biometrics and BEI into the intelligence process.
UNCLASSIFIED

Introductory table 1. (U) Summary of changes (continued)

Chapter 3—Plan and Direct
Chapter 3 is a revision of chapter 2 of the superseded manual. Additions include— • BEI support to steps 2, 3, and 4 of the military decisionmaking process. • BEI considerations during intelligence preparation of the battlefield.
Chapter 4—Collect
Chapter 4 is a revision of chapter 3 of the superseded manual. Additions include— • BEI support to information collection. • Cultural impacts of biometric collections. • Information on forensic functions and forensic-enabled intelligence. • Forensic support during offensive, defensive, and stability operations.
Chapter 5—Produce
Chapter 5 revises chapter 5 of the superseded manual. Additions include— • An update on BEI products. • Current biometric system screen shots.
Chapter 6—Disseminate
Chapter 6 revises chapter 6 of the superseded manual. Additions include an update on the biometric enterprise architecture.
Chapter 7—Analyze and Assess
Chapter 7 incorporates portions of chapters 5 and 6 of the superseded manual addressing the analysis and assessment of biometric information. The chapter includes— • A discussion on fusing BEI into all-source intelligence. • A Biometric Identity Intelligence Resource search screen example. • An update on analytic support tools.
Chapter 8—BEI Support to Decisive Action
• Chapter 8 is a new chapter. It contains a discussion of biometric and BEI support in offensive, defensive, and stability operations, and in defense support of civil authorities.
Chapter 9—BEI Considerations for Specific Operations, Missions, and Environments
Chapter 9 is a new chapter. It contains a discussion and supporting vignettes on various types of Army operations.
Appendix A—Biometric and BEI Resources
Appendix A is a revision of appendix A of the superseded manual. It adds an update on current biometric and BEI resources.
Appendix B—Biometric Modalities
Appendix B is a revision of appendix B of the superseded manual. It adds a discussion of tactics, techniques, and procedures for collecting biometric information of the various modalities.
Appendix C—Biometrically Enabled Watch List Categories (Tiers)
Appendix C is a new appendix. It contains an— • Update on biometrically enabled watch list tiers. • Update on Department of Defense-level biometrically enabled watch list categories and subcategories.
UNCLASSIFIED

Introductory table-2. (U) Summary of term changes

Term	*Remarks*
biometrics-enabled intelligence (Army)	Definition modified and source publication changed to ATP 2-22.82 vice ADRP 2-0.
UNCLASSIFIED	

PART ONE

Fundamentals (U)

Chapter 1

Overview (U)

(U) The use of BEI has been an integral force multiplier during counterinsurgency operations in Iraq and Afghanistan. The biometric techniques established in these theaters of operations led to the development of recognized Army BEI fundamentals that will continue to support commanders and the decisionmaking process. This chapter covers the fundamentals of BEI, including overviews of the biometric process, the BEI process, and BEI support to operations.

BEI ROLES AND RESPONSIBILITIES (U)

1-1. (U) Different organizations have specific roles and responsibilities pertaining to biometrics. Commanders at all echelons have a responsibility to integrate biometrics and BEI into operational and intelligence planning processes and cycles. Each organization is capable of contributing significantly to the repositories where identity characteristics are stored and retrieved to develop all-source intelligence. Biometrics and BEI are important aspects of this collection effort but are greatly enhanced when coupled with FEI, DOMEX, and other identity data. It takes a concerted focus from all organizations to synthesize these enablers into viable and mission critical intelligence products.

1-2. (U) Units leverage biometrics to the fullest extent possible to help defeat the enemy and enhance protection. Unit leaders and biometric collectors must understand that biometric data is shared and used globally across all DOD components, U.S. Government agencies, and in cooperation with international partners. Commanders must ensure the proper command emphasis, prioritization, and resourcing of biometric training and operations.

1-3. (U) Quality collection of biometric information enhances force protection and mission success throughout the force by eliminating the anonymity of adversaries and their associated networks. Higher quality collection results in more efficient and credible databases requiring less effort from database managers to correct discrepancies and increases the likelihood of successful matches. Leadership can support biometrics by—

- Ensuring training, operational planning, and mission execution incorporate biometric processes and proven techniques and procedures.
- Stressing the importance of quality over quantity in collections. Leaders stress standardized proper collection techniques throughout the biometrics community so analysts and decisionmakers can access credible data. An improper biometric collection wastes time and leads to gaps in knowledge, which may be exploited by the enemy.

- Providing feedback to collectors on the impact of their collections at tactical, operational, and strategic levels. In select areas, near real-time responses may be available to units in contact.
- Understanding the current rules of engagement and legal aspect of collecting biometrics. This will ensure effective use of biometrics during host nation legal proceedings.
- Considering proper site selection for biometric enrollment operations:
  - Select a location which supports the flow of personnel, type of operation, security considerations, biometric task (enrollment, identification, or verification), expected number of operators or collectors and enrollees, user circumstances, existing data, type and amount of equipment, and so forth.
  - Ensure adequate networks and communications are available to support the needs of the operation, which could vary from a host-nation (nonauthoritative) match to direct match against a multinational (authoritative) database.
- Including biometric capabilities in the unit's preexecution checklist. Leaders check to ensure all collection devices are loaded with the most up-to-date biometrically enabled watch lists (BEWLs) according to the unit's standard operating procedures and as operations dictate. At a minimum, the BEWL is updated weekly on the devices, but daily is preferred. (See paragraphs 5-31 through 5-39 for information on BEWLs.)
- Working closely with the multinational partners in the unit's area of operations, gaining their acceptance and support of biometric enrollment operations.

1-4. (U) For more information on the description of biometric roles and responsibilities, see DODD 8521.01E, and DODI O-3300.04.

FUNDAMENTAL BIOMETRIC TERMS (U)

1-5. (U) Joint doctrine defines *biometrics* as the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). A *biometric* is a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. Thus, the term biometrics designates both characteristics of an individual and a process. As a process, *biometrics* consists of the automated methods used to recognize an individual based on measurable *biometric* characteristics. This manual uses *biometrics* to indicate this process.

1-6. (U) The totality of an individual's biometric characteristics is that person's *biometric identity*. A biometric identity is established by collecting and linking biometric characteristics. The combination of biometric characteristics possessed by any person is unique. This fact, combined with the current technological state of multimodal biometric collection devices, makes a biometric identity more likely to identify an individual than biographical characteristics alone. (The term biometric identity is normally used in conjunction with biometric files that have not been associated with a person by name.)

BIOMETRIC FILES AND THEIR COMPONENTS (U)

1-7. (U) A *biometric file* is the standardized individual data set resulting from one or more biometric enrollments. Data contained in a biometric file falls into the following categories:

- Biological characteristics.
- Biographical characteristics.
- Behavioral characteristics.
- Contextual data.

1-8. (U) A *biological characteristic* is an individual characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. Fingerprints and hand geometry are examples of biological characteristics. A biological characteristic is recorded in a biometric sample. (See paragraph 1-14.) A biometric enrollment may include multiple biometric samples. A biometric file may include samples from several biometric enrollments.

1-9. (U) *Biographical characteristics* are physical or nonphysical characteristics of an individual from whom the biometric sample has been collected. Biographical characteristics include the following: full name, age, height, weight, address, telephone number, email address, birthplace, nationality, education level, and group affiliations. These characteristics also include data such as the person's employer, security clearances, and financial and credit history. The biographical characteristics for foreign nationals in an area of operations include interactions with U.S. and multinational forces. Biographical characteristics are also called associated data.

1-10. (U) A *behavioral characteristic* is an attribute that can be learned or acquired over time, rather than one based primarily on biology. Examples are signature, keystroke dynamics, and gait.

1-11. (U) *Contextual data* are the elements of biographical characteristics and situational information (who, what, where, when, how, why) associated with an enrollment. Contextual data describes the context in which an enrollment occurred, such as at a checkpoint or during a cordon and search. The data also include whether the individual was alone or with others. Contextual data are also called situational data.

BIOMETRICS-ENABLED INTELLIGENCE (U)

1-12. (U) The Army defines ***biometrics-enabled intelligence*** **as intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements.** BEI attempts to reduce anonymity and positively identify individuals based on qualities that make someone unique. It is critical for analysts to understand that biometric information and BEI must be combined with all-source information and intelligence for a complete BEI picture. Within Army intelligence doctrine, BEI is a complementary intelligence capability.

BIOMETRIC SYSTEMS, BIOMETRIC DATA, AND BIOMETRIC MODALITIES (U)

1-13. (U) Biometric information is collected, stored, analyzed, and managed with biometric systems. A *biometric system* is a grouping of multiple individual components (such as a sensor, matching algorithm, and result display) combined to perform a task related to collecting or supporting analysis of biometric data. A biometric system may be a component of a larger system. A biometric system is automation that may be capable of—

- Capturing a biometric sample from an individual.
- Extracting and processing the biometric data from that sample.
- Storing the extracted data in a database.
- Comparing the biometric data with data contained in one or more references.
- Determining how well the samples match and indicating whether an identification or verification of identity has been achieved.

1-14. (U) *Biometric data* is computer data created by biometric systems during an enrollment, verification, or identification process. Examples are raw sensor observations, biometric samples, models, templates, and similarity scores. Biometric data designates data about an individual collected during an enrollment, verification, or identification process. It does not pertain to information about users of that information, such as user name, demographic information, and authorizations. A *biometric sample* is data representing a biological characteristic of a person as captured by a biometric system.

1-15. (U) The categories of biometric data are called modalities. A *biometric modality* is a type or class of biometric sample originating from a person. During a biometric enrollment, each collected modality constitutes a separate sample. Said another way, a biometric enrollment normally consists of multiple biometric samples. The most commonly collected modalities are facial images, fingerprints, and iris images. Other modalities include—

- Voice recognition.
- Retina image.
- Hand geometry.
- Palm prints.
- Gait (manner of walking).
- Handwriting.
- Vascular mapping.

THE BIOMETRICS COMMUNITY (U)

1-16. (U) Supporting the other Services is a critical component of the Army's contribution to unified action. Army biometric and BEI development supports and aligns with joint identity intelligence operations. (See JP 2-0 for more information on identity intelligence.)

1-17. (U) The biometrics community includes all the entities and organizations with an interest in the development and utilization of biometrics. The community also includes all the Services, other U.S. Government agencies, and international partners. Every member of the community helps integrate biometric information into identity transactions needed to support military operations and departmental business functions. The current DOD biometrics enterprise strategic plan provides additional information on integrating biometrics into military operations. Institutionalizing biometrics into military operations enables unity of effort through sharing of biometric information, best practices, and lessons learned. Figure 1-1 shows the supporting biometrics community relationships and goals. The integration and utilization of biometrics by DOD organizations must include efforts to share data in order to be completely successful and support future biometric activities.

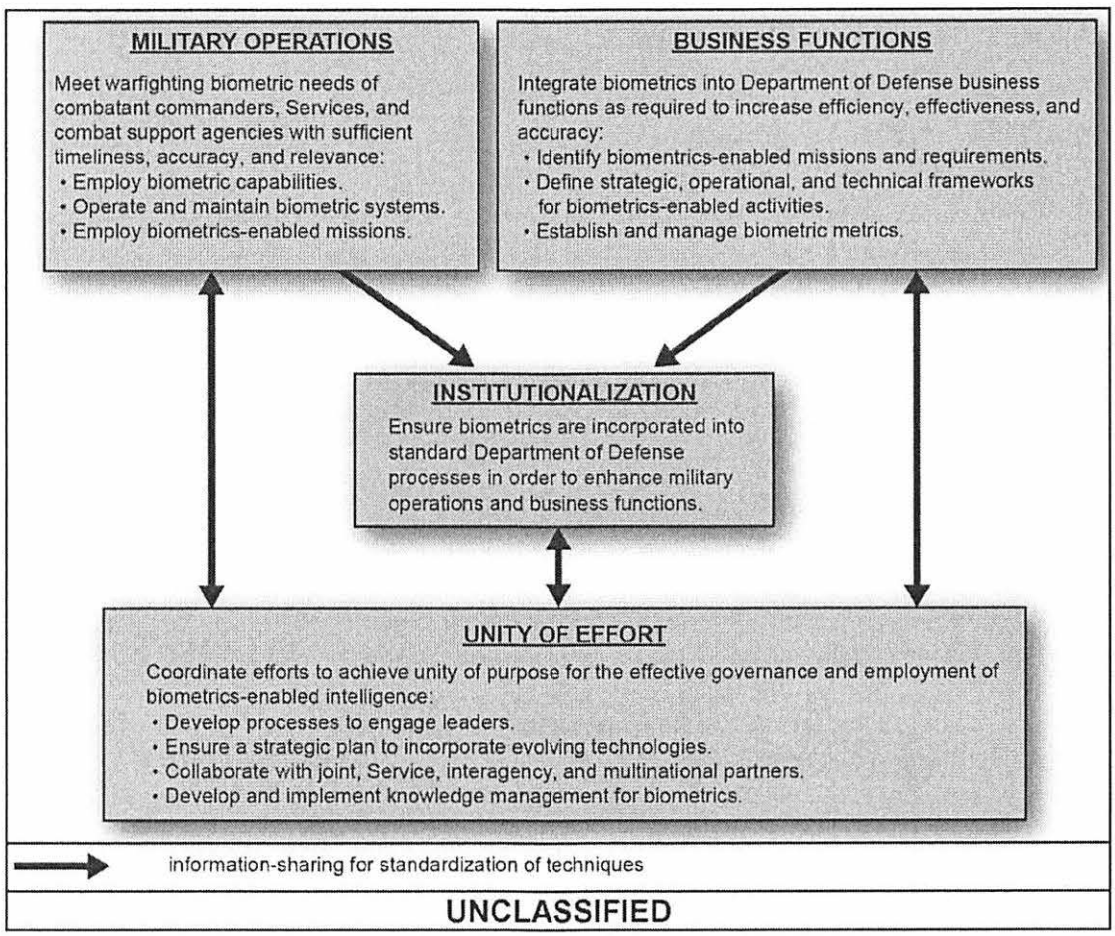


Figure 1-1. (U) DOD biometrics community goals and relationships

BEI WITHIN THE INTELLIGENCE PROCESS (U)

1-18. (U) BEI relies on information and intelligence data—as well as a distinct processing, exploitation, reporting, and dissemination enterprise—to integrate biometric information into the overall intelligence picture. This integration occurs during all steps and activities of the intelligence process. Biometric information comes from U.S. and non-U.S. collection and processing capabilities and is fused with, all-source intelligence and other information. Commanders use this information, and the intelligence gained from it, to monitor or neutralize the influence and operational capacity of threat individuals, cells, and networks of interest trying to operate anonymously. (See chapter 2 for more details on the BEI process.)

1-19. (U) BEI provides commanders the capability to positively identify threat individuals and deny threat anonymity. BEI remains an integral piece of all-source intelligence and operational success in all environments.

PLAN AND DIRECT (U)

1-20. (U) During the planning and directing activity, the intelligence staff identifies and advises the commander on where biometric collections would be beneficial and what BEI products can help achieve mission success. As the courses of action mature, the intelligence staff identifies BEI requirements, prioritizes them, and integrates them into the commander's information and intelligence requirements. The biometric-specific collection requirements are then incorporated into the unit information collection plan and follow-on collection plans to help focus biometric collection efforts. (See FM 3-55 for additional details on information collection. See ATP 2-01 for doctrine on planning requirements.)

1-21. (U) During planning and directing, rules for processing and exploiting biometric data are developed or updated for the range of military operations and all decisive action tasks (offense, defense, and stability). Likewise, specific BEI production requirements are identified, as well as rules and guidance for disseminating and integrating BEI into future intelligence requirements and unit plans. (See chapter 3 for information on incorporating biometric activities into intelligence planning and direction.)

COLLECT (U)

1-22. (U) Collection managers ensure the collection of biometric information, which ultimately leads to BEI, is part of the planning and collection processes. Collection is synchronized to provide critical information at key times throughout the phases of an operation and during the transition from one operation to another operation. A successful biometric collection effort results in the timely collection and reporting of relevant and accurate information, which supports the production of intelligence. Army biometric data collection capabilities are constantly evolving, becoming more versatile, detailed, and reliable. (See chapter 4 for information on biometric collection.)

PRODUCE (U)

1-23. (U) Production is the development of intelligence through the analysis of collected information and existing intelligence. To answer requirements, analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment in an effective format. Intelligence products must be timely, relevant, accurate, predictive, and tailored to facilitate situational understanding and support decisionmaking. The accuracy and detail of intelligence products have a direct effect on operational success.

1-24. (U) Accessible databases store biometrics and related data for use by analysts during intelligence production to enhance situational awareness. Analysts at all echelons generate BEI products that support and meet a commander's information and intelligence requirements. Analysts not only tailor BEI products to the needs of the commander but also prepare reports that are releasable to the lowest possible echelon, multinational partners, or the host nation. (See chapter 5 for information on BEI production.)

DISSEMINATE (U)

1-25. (U) Most intelligence disciplines utilize dissemination and integration systems or processes to push information to those who need it. Analysts share and retrieve biometrics via secure and nonsecure Web-enabled portals. Users feed biometric data through the biometric architecture to local or regional servers. Analysts and organizations support commanders as they integrate information and intelligence into their decisionmaking and planning processes. Most non-military-intelligence personnel do not have access to U.S. Government biometric databases. Echelon intelligence officers must develop alternative methods to get critical, time-sensitive biometric information to the right personnel, at the right time, and in a useable format.

1-26. (U) BEI dissemination and analytical integration does not cease when BEI products are posted to a database. Commanders ensure the integration of BEI products into future intelligence operations. These products, along with a robust collection effort, significantly supplement the targeting process. (See chapter 6 for information on BEI dissemination.)

ANALYZE AND ASSESS (U)

(b) (3)

1-28. (U) The analysis activity answers the intelligence *so what?* question behind the biometric encounter. It defines the intelligence value of the information gathered. Because it is a human function performed by an analyst, the analyzing activity is not an automated biometric enterprise core capability. Nevertheless, it lies at the heart of the BEI process.

1-29. (U) BEI contributes to all-source analysis and is incorporated into intelligence products in order to provide the commander with a clearer intelligence picture. Additionally, BEI is incorporated to satisfy the commander's critical information requirements concerning persons, networks, or populations of interest. BEI analysis begins in response to the results of the biometric comparison or to a requirement to find a biometric sample for a person of interest.

1-30. (U) The assessing activity is continuous throughout the intelligence process and asks such questions as—

- Are unit intelligence activities directed at answering the commander's intelligence requirements?
- Are biometric concerns and capabilities being addressed and used effectively?
- Are collection assets being utilized effectively to answer intelligence requirements?
- Is biometric data being processed and analyzed in a timely manner and to support operational needs, including targeting?
- Are biometric architectures being utilized effectively?

1-31. (U) This list is not all inclusive, but analysts should always assess if intelligence activities are effective and if they are producing the results that the commander needs. (See chapter 7 for information about analyzing and assessing biometric activities.)

BIOMETRICS AND BEI IN EMERGING DOCTRINE (U)

1-32. (U) As the Army continues to look to the future, there is an uncertain strategic environment that will challenge all Soldiers, leaders, and organizations in many ways. Future adversaries are likely to be highly adaptive and occupy an environment that greatly complicates the ability of Army forces to conduct operations. They will most likely attempt to deny U.S. and multinational forces access to their territory. When friendly forces do gain access, adversaries will attempt to deny those forces freedom of movement. This environment will require friendly forces to conduct expeditionary operations, operations in large urban areas, and operations with reduced military resources. A significant part of these operations will include various biometric and BEI activities.

1-33. (U) The United States anticipates an expanding range of smaller, shorter, rapidly changing missions in which adversaries attempt to hide within the greater populace. These missions are compelling the Army toward superior agility, expanded expeditionary capabilities, precise lethality, special operating force and conventional force interdependence, a greater capacity for theater security cooperation, and improved cultural awareness. Many recent adversaries have attempted to operate anonymously against U.S. and multinational forces. Biometrics and BEI are key contributors to identifying, locating, and targeting these adversaries. Specifically, analysts use the BEI process to satisfy requirements involving the location, activities, or other issues concerning specific people or groups of people. Therefore, partnering with other countries and building the biometric and BEI capacity of regionally aligned U.S. and multinational forces is important during theater security cooperation (also called TSC) activities.

1-34. (U) Biometrics and BEI are critical to future operations for a number of reasons:

- They are the primary source of information commanders and other consumers use to positively identify specific individuals or groups of people.
- They help analysts develop insight into threat individuals, enemy groups and organizations, and threat characteristics and patterns.
- They support the protection warfighting function by helping to ensure only positively identified, and appropriately authorized, locally employed persons and third-country nationals are allowed entry onto bases and other friendly facilities.

BIOMETRICS AND BEI DURING THE PHASES OF OPERATIONS (U)

1-35. (U) Army forces—as part of joint, interagency, intergovernmental, and multinational teams—protect the homeland and engage regionally to prevent conflict, shape security environments, and create multiple options for responding to and resolving crises. Mission-tailored Army units are regionally engaged across the globe, building partners, deterring adversaries, and overcoming challenges to defeat enemies using multiple, often simultaneous, actions integrated in time, space, and purpose. The joint force commander and Service component commanders arrange operations and activities through the joint phasing model (joint phases of operations). (See JP 3-0.) There are six phases:

- Shape (phase 0).
- Deter (phase 1).
- Seize the initiative (phase 2).
- Dominate (phase 3).
- Stabilize (phase 4).
- Enable civil authority (phase 5).

1-36. (U) There are requirements for biometric information and BEI during each phase. Some biometric and BEI activities are specific to certain phases, while others span multiple phases. Commanders and other leaders address the collection, storage, processing, exploitation, and dissemination of biometric information and associated contextual data in each phase. Commanders remain aware that some biometric activities are performed during multiple phases of some operations. These biometric activities support the continuous and worldwide analysis of that data and development of BEI. All regional biometric activities must be

synchronized with the Department of Defense Automated Biometric Identification System (ABIS). (ABIS is DOD's authoritative biometric database.)

1-37. (U) Ideally, regionally aligned forces develop and populate a local database of biometric signatures and associated contextual information during phase 0. The database can then be maintained and continually populated during all subsequent phases. However, units will not always be able to establish the database during phase 0. Therefore, commands prepare to establish localized biometric databases during any phase of an operation. It is critical for commands to continuously update the biometric database of actual and potential adversaries to maximize the value of BEI.

PHASE 0—SHAPE (U)

1-38. (U) In the *shape* phase, the command focuses on building the biometric, BEI, forensics, and FEI capacities of U.S. and multinational forces and on demonstrating to multinational partners the value of sharing biometrics-related information. Some possible biometric and BEI activities include—

- Developing and establishing agreements, policies, and regionally aligned forces' relationships for collecting, storing, accessing, and sharing biometric data, as well as associated contextual data, required for operational use and for the development of BEI. Commands ensure this is coordinated with and among Army, joint, and multinational forces, and with U.S. Government agencies.
- Developing the architectures necessary to support the agreements, policies, and regionally aligned forces' relationships pertaining to biometrics and BEI. Commands ensure the architectures provide for the integration of new information into all standing databases, such as those from the Federal Bureau of Investigation (FBI), Department of Homeland Security, and the International Criminal Police Organization (Interpol).
- Conducting basic biometric training with multinational and interagency partners, including what biometrics is, how to collect and store biometric data, and how to use the BEWL. (See paragraphs 5-31 through 5-39 for information on BEWLs.)
- Researching and analyzing potential areas of operations to determine what biometric databases, such as any within local police forces or other host-nation governmental agencies, are in use and how they can be accessed.
- Beginning to identify information requirements involving the location, activities, or other issues concerning a specific person or group that can be satisfied through the use of biometrics and BEI.
- Establishing a preliminary local biometric database, when feasible.
- Beginning the process of identifying actual and potential enemy personnel for nomination to and inclusion in regional BEWLs.
- Identifying and incorporating biometric manning, collecting, storing, accessing, and sharing requirements into contingency plans.

PHASE 1—DETER (U)

1-39. (U) During the *deter* phase, the increased use of biometric collection systems by multinational forces or DOD personnel and the subsequent analysis and sharing of BEI provide an elevated security posture for the United States and partner nations. The security effort is supported by placing biometric enrollments collected by multinational forces into the DOD authoritative biometric database (ABIS). Matches to watch lists and persons of interest are provided to multinational partners.

1-40. (U) Some possible biometric and BEI activities include—

- Coordinating with joint forces, other U.S. Government agencies, and multinational forces to execute the agreements, architectures, and policies for biometrics and BEI development. Commands ensure architectures provide for integration of new information into all standing databases, such as those from the FBI, the Department of Homeland Security, and Interpol.
- Continuing to use biometrics and BEI to assist in identifying and focusing information requirements involving the location, activities, or other issues concerning specific persons or groups.
- Continuing to identify enemy and potential enemy personnel for nomination to and inclusion in regional BEWLs.
- Coordinating with joint forces, other U.S. Government agencies, and multinational forces to begin full biometric enrollments of specific individuals and types of people within the area of operations.
- Beginning the development of BEI for use in the overall intelligence process and the development of all-source intelligence products.
- As appropriate, sharing biometric data and BEI with joint forces, other U.S. Government agencies, multinational forces, and other communities of interest.
- If authorized, using information from current authoritative source databases (see paragraph 7-19) to assist in identifying, locating, and targeting of persons of interest.

PHASES 2 AND 3—SEIZE THE INITIATIVE AND DOMINATE (U)

1-41. (U) During the *seize the initiative* and *dominate* phases, units conduct biometric enrollments of persons encountered on the battlefield when the tactical situation permits. Additionally, commanders can use this same biometric and forensic information, coupled with other identity data, to support military criminal or war crime prosecutions. Enrolling detainees and key segments of the local population as the tactical situation permits not only allows for better control of detained personnel but also facilitates the later identification of people who may become hostile. Conducting increased enrollments and identifications also provides for the security of the local populace by demonstrating the ability to positively identify individuals across time and space regardless of their method of disguise.

1-42. (U) Some possible biometric and BEI activities include—

- Supporting the targeting of high-value individuals and other persons of interest in support of—
  - Operations at the tactical and operational echelons.
  - National and multinational authorities.
- Assisting in the positive identification and control of—
  - Detainees and other persons of interest.
  - Civilians at critical points throughout the area of operations, especially at checkpoints.
  - Personnel during cordon and search operations.
  - Personnel at key local infrastructure facilities, such as communications nodes, power stations and substations, and water and sewage facilities.
- Enhancing overall population management by providing friendly forces a significant means to positively identify foreign fighters, insurgents, and other nonindigenous people.
- Supporting detention and interrogation operations.
- Aiding in the positive identification of isolated personnel returned during personnel recovery operations. (See FM 3-50 for personnel recovery doctrine.)

PHASES 4 AND 5—STABILIZE AND ENABLE CIVIL AUTHORITY (U)

1-43. (U) The continued use of biometric and BEI activities introduced in earlier phases aids U.S. and multinational forces in the continued identification, locating, and targeting of threat personnel during the *stabilize* and *enable civil authority phases*. Full integration of biometric activities into daily patrols,

security screenings, tactical checkpoints, cordon and search operations, and other activities also contribute to accomplishing these tasks. As the tempo of operations slows and the transfer of authority to civil authorities occurs, the use of biometrics and BEI shifts from controlling the populace and identifying threat personnel to facilitating the resumption of more normal, peacetime activities.

1-44. (U) Some possible biometric and BEI activities include—

- Supporting security at key leader engagements. (See FM 3-53.)
- Enhancing a commander's understanding of population attitudes toward U.S. and multinational forces by assisting in positively identifying members of the populace who do and do not support friendly forces.
- Contributing to the establishment of a safe and secure environment by assisting in the identification of individuals, or groups of individuals, who do not desire to see an end to hostilities.
- Providing the positive identification of members of the local populace necessary to assist in establishing essential governmental services, emergency infrastructure reconstruction, contract and monetary disbursements, and humanitarian relief.
- Enhancing the positive identification of personnel in support of—
  - Detainee operations.
  - Personnel recovery operations.
  - Operations at ports of entry.
- Enhancing the identification of deceased high-value targets.
- Enhancing the vetting of personnel hired into host-nation government organizations, such as police forces and health services agencies, government-controlled facilities, and other infrastructure.

Chapter 2
Biometric Processes (U)

(U) This chapter describes automated and manual biometric processes that enable analysis. The chapter also discusses how biometric data is processed in biometric systems. Additionally, the chapter addresses the steps involved in developing BEI.

THE BIOMETRIC AUTOMATED PROCESS (U)

2-1. (U) Analysts who understand the biometric automated process significantly increase their unit's analytical capabilities by ensuring the integration of biometrics into the operations and intelligence processes. In addition to understanding how biometrics are processed in automated systems, analysts need to know how to properly incorporate biometric data into all intelligence process steps and activities, thus enabling a better understanding of the operational environment.

2-2. (U) Biometric automated actions combine to form a process by which biometric data can be automatically processed and stored in a national repository for retrieval by analysts throughout DOD. The biometric automated process comprises four automated actions: normalize, match, store, and share. (See figure 2-1.) These actions occur when data is entered into a biometric collection device or stored in a biometric repository. Each action is an integral part of the automated process and a building block for the following action. Each action ensures the biometric data follows a specific path to the repository and allows analysts to retrieve the data and manipulate it into various BEI products. The data is shared with interagency departments daily and may be shared with partner nations on a case-by-case basis.

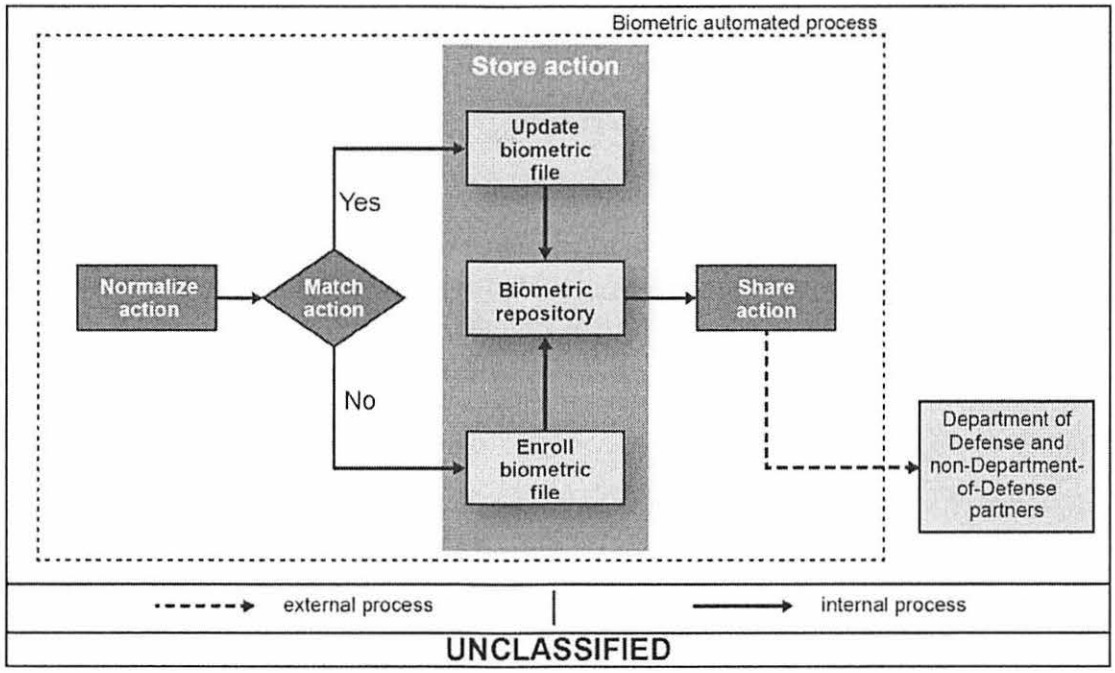


Figure 2-1. (U) The biometric automated process and its component actions

Note. (U) Throughout the biometric automated process and BEI process, commanders and leaders must ensure operations are conducted in accordance with applicable laws, policies, authorities and agreements.

NORMALIZE (U)

2-3. (U) *Normalization* is the process of transforming one or more biometric samples from a single person into a single biometric file of standard format meeting a specified quality level. This ensures biometric files are easily shared and used by the automated biometric systems of DOD and other agencies. The normalize action results in a standardized, high-quality biometric file consisting of a biometric sample and contextual data.

2-4. (U) DOD biometric collection systems are generally capable of creating normalized biometric files at the point of collection. However, biometric files obtained from other countries are likely to have contextual data written in a foreign language and use formats incompatible with DOD systems. Manual normalization is time consuming and resource intensive but is critical for updating and populating biometric repositories.

2-5. (U) Once a biometric file is normalized, it is transmitted to a data source for matching, if the biometric collection system does not allow for matching at the point of collection. The normalize action of the biometric automated process correlates with the produce step of the intelligence process.

MATCH (U)

2-6. (U) The match action determines whether different biometric samples come from the same person, based on their level of similarity. Matching can be performed to determine either biometric identification or biometric verification:

- *Biometric identification* is 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.
- *Biometric verification* (also called biometric authentication) is the automated process of comparing a submitted biometric sample against one biometric file (one-to-one) to determine if they match.

2-7. (U) Matching begins with receipt of a collected, normalized biometric sample. It continues with the biometric system comparing the sample with biometric files in the supporting biometric repository. The collector is notified by a prompt on the collection device showing the results of the comparison. (The exact prompt depends on the system in use.) The collector then makes a decision regarding the disposition of the individual who provided the biometric sample.

2-8. (U) An important component of matching is the system threshold score, which is a setting for some biometric systems that can compare biometric samples. The acceptance or rejection of biometric data depends on the match score falling above or below the formatted threshold. The threshold is adjustable, which allows the biometric system to be more or less strict, depending on requirements.

2-9. (U) Enrolling the biometric sample and other data into a repository as a new biometric file, or updating the repository file, completes the matching process. Even though biometric data is being compared with other biometric data in an automated system and not by an analyst, the matching action of the biometric automated process correlates with the continuing activity of analysis that occurs throughout the intelligence process. However, relevant data from the repository needs to be assessed by an analyst to ensure it makes sense based on the current operational situation. This assessment may occur during matching or later, depending on the urgency of the situation.

STORE (U)

2-10. (U) The store action makes standardized and current biometric data available for all analysts to access at any time. An individual's biometric file is stored in the biometrics repository. Upon subsequent

encounters, the individual's file is updated each time with additional data. Depending on the operational requirements and environment, the storing action may occur in a local biometric database on a laptop computer, at a large data center in a theater of operations storage node (consisting of a server within a secure location), in a national database, or in all three.

2-11. (U) The store action of the biometric automated process correlates with the continuing activity of analysis and the production step of the intelligence process. Even if biometric data does not have immediate value, it is stored for future use. That way, it can be accessed and compared or analyzed whenever necessary to support intelligence activities. Moreover, the data can be used as part of intelligence products to support answering intelligence requirements.

SHARE (U)

2-12. (U) The share action is the exchange of normalized biometric files and match results among approved DOD, interagency, and multinational partners in accordance with applicable laws, policies, authorities, and agreements. Unfiltered and unanalyzed biometric data may be shared among databases. Building sharing relationships with other units, Services, and countries allows more effective use of biometric information and contributes to developing better BEI.

2-13. (U) Sharing biometric data is authorized among Army-, DOD-, and intelligence community-approved repositories to ensure agencies across the intelligence enterprise have access to the same information. The share action of the biometric automated process correlates to the disseminate step of the intelligence process. (See DODD 8521.01E for policy on the integration and coordination of biometric products, systems, and services throughout DOD.)

THE BEI PROCESS (U)

2-14. (U) Biometric information that has been through the automated process is exploited to create BEI. However, biometric information alone does not create BEI; it must be synthesized with other intelligence and information to have full value and relevance. To create BEI products, analysts retrieve and analyze biometric files containing biometric data and biographical and behavioral characteristics, before synthesizing them with other all-source information. (See figure 2-2 on page 2-4.)

2-15. (U) The BEI process aligns with the BEI definition. It has four components:

- Biometric and associated data.
- Intelligence data and reporting.
- Operational environment data.
- Commander's intelligence requirements.

BIOMETRIC AND ASSOCIATED DATA (U)

2-16. (U) Biometric data consists of collected biometric characteristics, such as fingerprints, iris images, or palm prints. Each of these provides unique and specific identifiers for an individual. This data is compared to other data to determine a possible match.

2-17. (U) *Associated data* (also called biographical characteristics) are physical and nonphysical attributes of an individual from whom the biometric sample has been collected. These are nonbiometric attributes that provide some identifying information about an individual but lack the distinctiveness and permanence to differentiate any two individuals. These include the following data about a person: height, weight, gender, eye color, nationality, ethnicity, personal habits, age, resident addresses, employers, telephone numbers, email address, place of birth, family names, education, security clearances, and financial and credit history. Associated data are extremely valuable because they add context to the biometric data, possibly providing a better understanding of a person of interest.

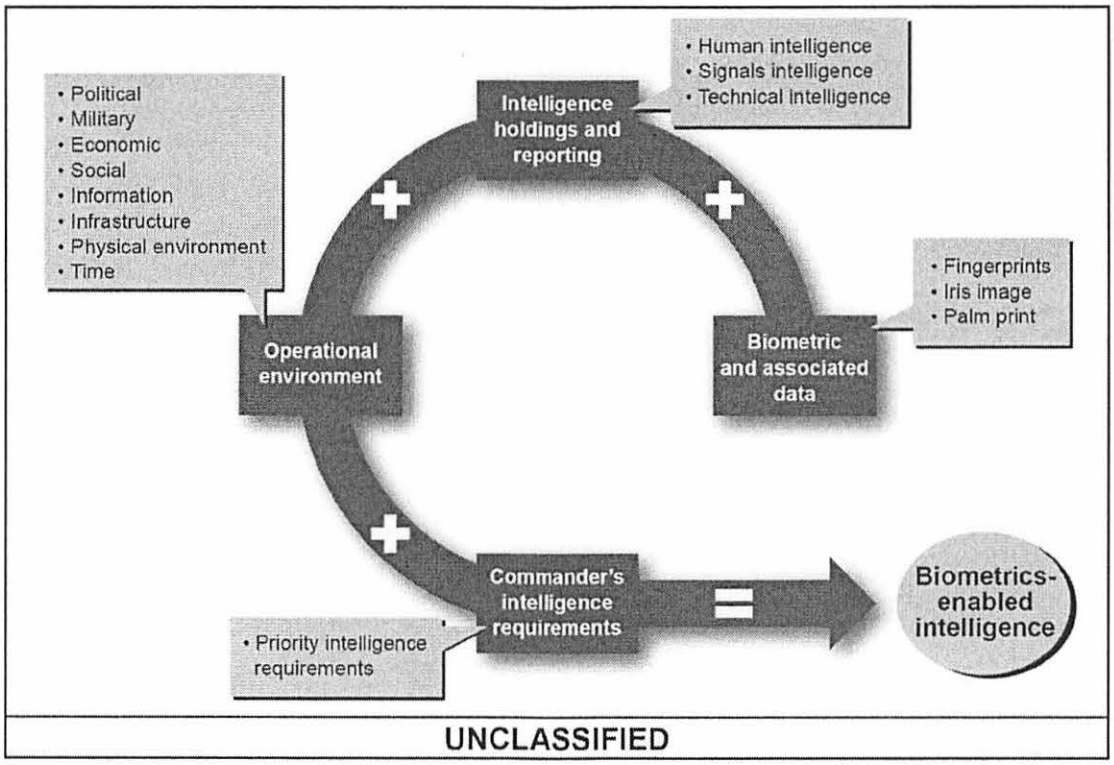


Figure 2-2. (U) The BEI process

INTELLIGENCE HOLDINGS AND REPORTING (U)

2-18. (U) In order to fully understand and exploit biometric and associated data, an analyst evaluates them in relation to other intelligence and reporting.

BEI Development Vignette (U)

(b) (3)

OPERATIONAL ENVIRONMENT (U)

2-19. (U) Understanding the operational environment is imperative to all aspects of military operations. Army planners analyze an operational environment in terms of the operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (also called PMESII-PT). (See ADRP 5-0 and ATP 2-01.3/MCRP 2-3A.) By focusing intelligence efforts on the operational variables, an analyst acquires knowledge the intelligence staff needs to better plan biometric collection activities and add meaning to biometric data collected.

BEI Development Vignette (continued) (U)

(b) (3)

(U) Study of the operational environment, along with biometric information and other intelligence, enables the analyst to recommend a closer study of the person of interest, religious leader and building, and suspected threat house.

COMMANDER'S INTELLIGENCE REQUIREMENTS (U)

2-20. (U) One of the intelligence staff's main roles is to answer the commander's intelligence requirements. By combining biometric information with other information and intelligence, the BEI process helps analysts answer intelligence requirements. Understanding the commander's intelligence requirements and synchronizing intelligence activities to meet them supports successful mission accomplishment.

BEI Development Vignette (continued) (U)

(b) (3)

INCORPORATING BIOMETRIC PROCESSES INTO THE INTELLIGENCE PROCESS (U)

2-21. (U) 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. The all-source approach enables analysts to provide clarity to an otherwise ambiguous battlefield that includes friendly, neutral, and hostile individuals occupying the same space and time. The requirements for collecting biometric information and synchronizing collection capabilities are integrated into the intelligence process. The continuous intelligence activities of analyze and assess must be part of this integration as well. The BEI process provides a framework for analysts and leaders to logically integrate biometrics and associated capabilities into each step of the intelligence process.

2-22. (U) Analysts use biometric information throughout the intelligence process to help answer the commander's intelligence requirements. The final step of the intelligence process, dissemination, provides the commander with BEI products and recommendations for specific courses of action concerning persons of interest. These recommendations are implemented by updating the BEWL, developing the situation map, or recommending that an individual be added to the BEWL. Figure 2-3 on page 2-6 depicts how the biometric processes are integrated into the intelligence process to produce BEI for the commander. When executed correctly, integrating biometrics into the intelligence process enables commanders to have a better

understanding of the operational environment. (See paragraphs 5-31 through 5-39 for information on BEWLs.)

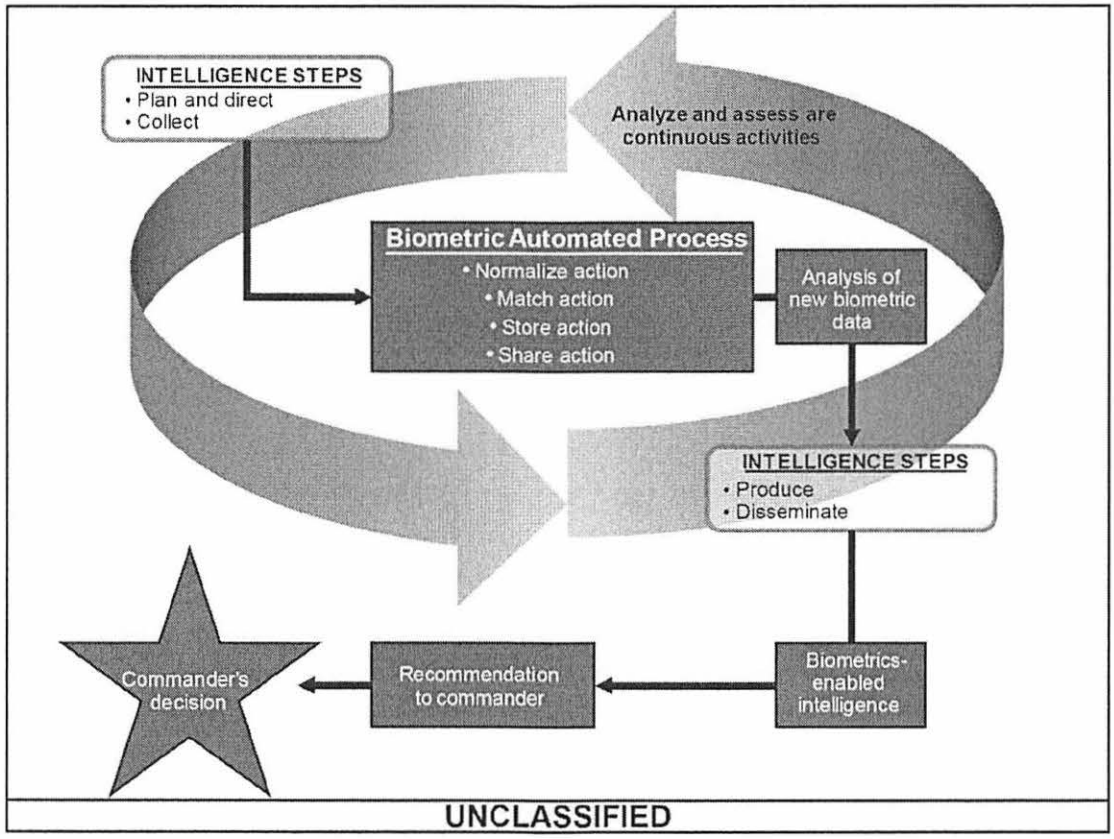


Figure 2-3. (U) Integrating biometrics into the intelligence process

PART TWO

Biometrics and the Intelligence Process (U)

Chapter 3

Plan and Direct (U)

(U) Early and thorough planning and directing is the foundation for effectively integrating BEI into all aspects of an operation. BEI requirements concerning persons, networks, and populations are submitted during planning requirements and assessing collection to ensure BEI requirements are included and answered as the operation is executed. (See ATP 2-01.) BEI is incorporated into planning as early as possible to ensure the appropriate integration and synchronization of collection requirements for the operation.

ADVANTAGES OF PLANNING AND DIRECTING (U)

3-1. (U) Army design methodology and the military decisionmaking process (MDMP) are supported by and drive considerations for intelligence planning. Planning and directing provides—

- Validated and prioritized information, collection, and production requirements.
- A strategy for executing biometric collection that is synchronized with the supported command's concept of operations.
- A strategy for processing and exploiting collected biometric and contextual data.
- BEI analysis and production planning.
- BEWL nomination instructions, screening criteria, and a management structure. (See paragraphs 5-31 through 5-39 for information on BEWLs.)
- Strategies for data dissemination and information-sharing.
- A BEI architecture, including databases, dissemination means, and analytical tools.
- Measures of performance, measures of effectiveness, and mechanisms to capture assessments and provide feedback.
- Recommendations for tasking to organic and supporting assets.

PLANNING CONSIDERATIONS (U)

3-2. (U) Utilizing information and intelligence already available saves valuable time when integrating BEI into planning. Some biometric resources to use while gathering information on persons of interest or groups include—

- U.S. databases, such as the Biometric Identity Intelligence Resource (also called the BIIR). (See paragraph 4-21.)
- Multinational biometric data (requires requests for information and special coordination).
- Host-nation biometric information (requires requests for information and special coordination).

3-3. (U) Considerations for planning include the status of individuals that forces encounter. Biometric collectors categorize individual identities by status, which determines how the data is processed based on laws, policy, social convention, and security requirements. There are three accepted statuses:

- **Friendly**—trusted individuals, DOD personnel and family members, U.S. persons, trusted allies, and multinational partners.
- **Neutral or unknown**—nonaligned individuals, host-nation, and third-country nationals.
- **Adversary**—enemy combatants, known or suspected terrorists, detainees, criminals, hostile foreign intelligence officers, and persons of interest.

3-4. (U) Another planning consideration is the type of operation the supported unit is conducting. Generally, any situation in which Soldiers encounter individuals not explicitly known to be friendly is an opportunity for biometric collection or identity verification, for example—

- Detainee management.
- Base or building access control.
- Population screening.
- Civil and governmental activities.
- Civilian, military, or community leader assessments.

3-5. (U) Biometric and BEI analysts need to be aware of all the planning tools available to them as they conduct IPB. Planning tools that support biometrics and BEI include—

- Event template.
- Named areas of interest.
- Target areas of interest.
- Density plot overlays.
- Link diagrams.
- Battle damage assessment charts.
- The operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (also called PMESII-PT).
- Civil considerations: areas, structures, capabilities, organizations, people, and events (also called ASCOPE).

3-6. (U) The operational variables are fundamental to developing a comprehensive understanding of an operational environment. Civil considerations help analysts better understand the local culture in the operational area. (See ADRP 5-0 and ATP 2-01.3/MCRP 2-3A.)

3-7. (U) The use of these and other intelligence tools during planning provide intelligence professionals and commanders at all levels with a better understanding of the operational environment, decreasing unknown factors and increasing the probability of mission success. (See paragraphs 7-32 through 7-41 for additional information on planning tools that support biometrics and BEI.)

BEI AND THE MILITARY DECISIONMAKING PROCESS (U)

3-8. (U) The *military decisionmaking process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The MDMP steps are—

- Receipt of mission.
- Mission analysis.
- Course of action development.
- Course of action analysis.
- Course of action comparison.
- Course of action approval.
- Orders, production, dissemination, and transition.

3-9. (U) The MDMP integrates the activities of the commander, staff, subordinate headquarters, and unified action partners to understand the situation and mission, develop and compare courses of action, decide on a course of action that best accomplishes the mission, and produce an operation plan or order for execution. This process helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. (See ADRP 5-0 and FM 6-0 for more information on MDMP.)

3-10. (U) During the MDMP, the intelligence staff is responsible for providing well defined, specific all-source intelligence products and tools. The staff tailors the all-source products and tools to the commander's requirements and the operation. All the MDMP steps are important and lead to a better understanding of the operational environment. However, it is critical for intelligence staffs to integrate biometric and BEI efforts into steps 2, 3, and 4.

STEP 2—MISSION ANALYSIS (U)

3-11. (U) Initial intelligence products are integrated into the MDMP during step 2. Intelligence requirements, an updated IPB, and running estimates are outcomes of this step. The more time and effort the intelligence staff can commit to thorough analysis before executing step 2, the better developed intelligence products they produce. Included in the analysis and research before step 2 are biometric databases, forensic databases, and BEI review of operational areas. Figure 3-1 depicts BEI considerations incorporated into step 2.

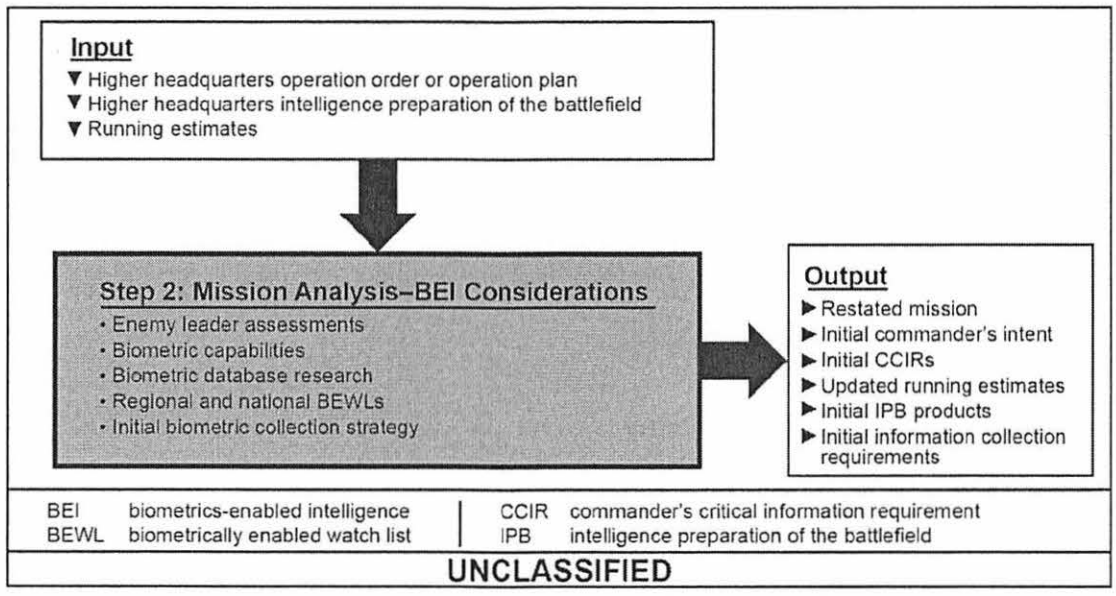


Figure 3-1. (U) BEI considerations during military decisionmaking process step 2

STEP 3—COURSE OF ACTION DEVELOPMENT (U)

3-12. (U) The purpose of course of action development is to update the running estimates and prepare options for the commander's consideration. The staff develops friendly courses of action based on facts and assumptions identified during IPB and mission analysis. Incorporating the results of IPB into course of action development ensures that each friendly course of action takes advantage of the opportunities the environment and threat situation offer and attempts to mitigate the most significant risks. (Figure 3-2 depicts BEI considerations incorporated into step 3.)

3-13. (U) Incorporating biometrics into step 3, course of action development is critical because it enables better biometric strategies to support operations. These strategies help determine needed biometric resources, collection plans, processing priorities, and dissemination architectures.

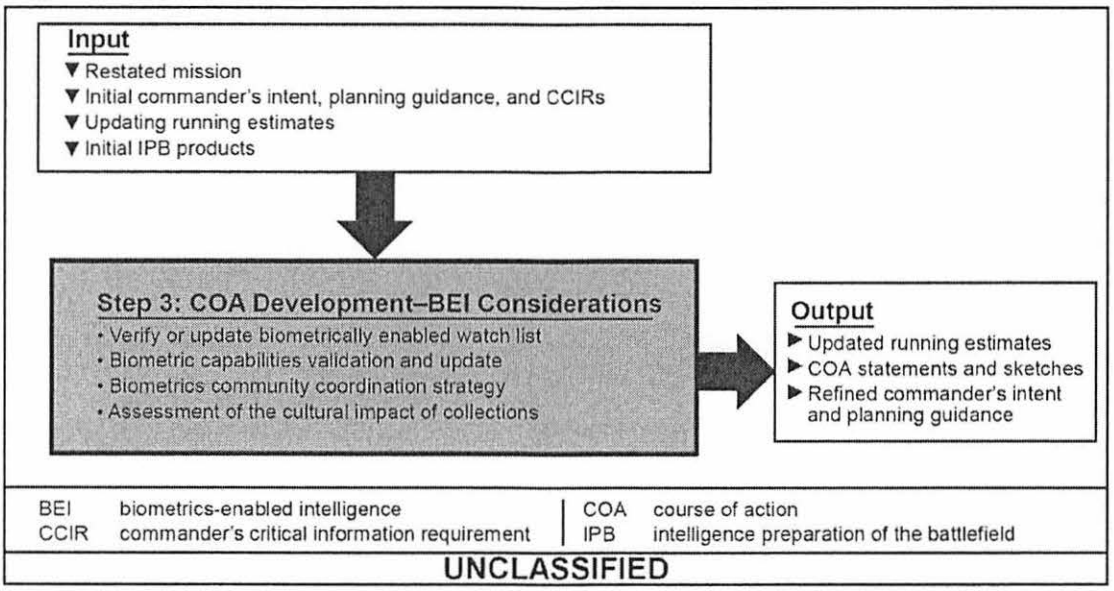


Figure 3-2. (U) BEI considerations during military decisionmaking process step 3

STEP 4—COURSE OF ACTION ANALYSIS (WARGAMING) (U)

3-14. (U) Step 4 of the MDMP is also critical to the success of operations. During this step, the intelligence staff continues to update all intelligence products and analyses, including biometric information and BEI and how they affect friendly operations. Additionally, intelligence personnel participate in wargaming, where they present possible threat actions and reactions to friendly operations. Included in wargaming are the threat's ability to counter biometric data collection, such as avoiding biometric collection efforts, removing fingerprints, or changing facial features. (Figure 3-3 depicts BEI considerations incorporated into step 4.)

BEI AND INTELLIGENCE PREPARATION OF THE BATTLEFIELD (U)

3-15. (U) *Intelligence preparation of the battlefield* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3/MCRP 2-3A). By applying IPB, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space.

3-16. (U) Biometrics and BEI contribute significantly to the refinement of IPB. Biometric information and the analysis provided by developing BEI can help locate the threat and identify threat characteristics.

3-17. (U) Intelligence planning is integrated into the entire MDMP. Early planning for biometric analysis and BEI integration includes support to IPB and development of all-source intelligence. Intelligence planners must understand the purpose, environment, and characteristics of—

- The MDMP. (See ADRP 5-0.)
- IPB. (See ATP 2-01.3/MCRP 2-3A.)
- Intelligence analysis. (See ATP 2-33.4.)

3-18. (U) Additionally, intelligence planners must understand—

- Enemy tactics.
- The enemy's ability to react to circumstances and friendly actions.
- The art of tactics. (See ADRP 3-90.)

3-19. (U) Before formal planning, the staff conducts extensive preparation and analysis to satisfy the requirements of IPB. Biometric information and BEI contribute to the overall intelligence picture, allowing intelligence staffs to better support commanders' planning and decisionmaking. During planning, the intelligence staff is responsible for developing a specific set of products and tools that support the MDMP. Preparation for incorporating biometric data and BEI into IPB occurs concurrently with other intelligence activities that contribute to IPB.

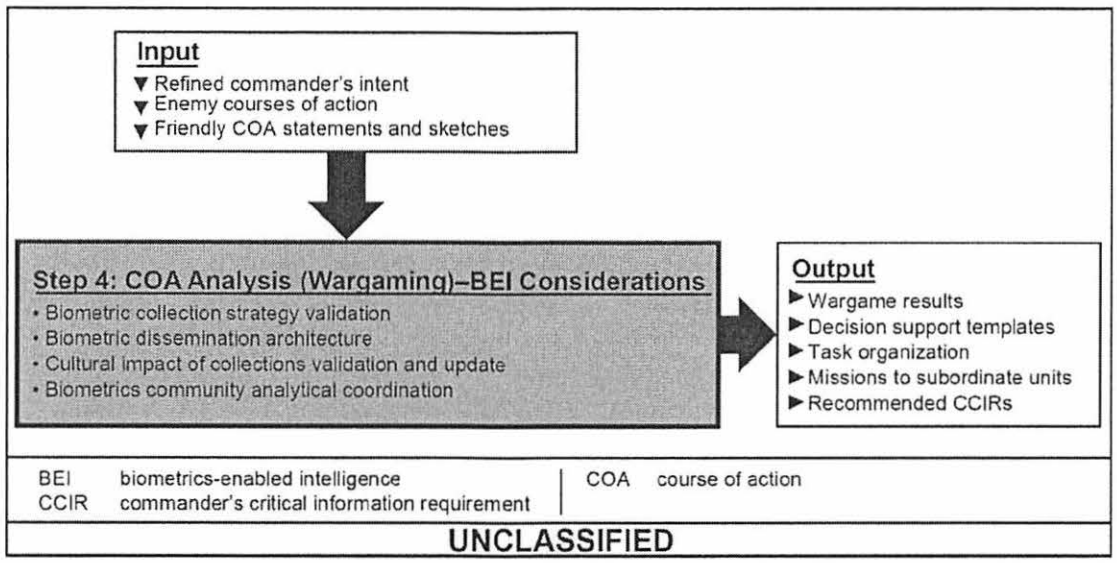


Figure 3-3. (U) BEI considerations during military decisionmaking process step 4

3-20. (U) Intelligence staffs identify BEI requirements and prioritize them along with the rest of the commander's information and intelligence requirements. The biometric-specific requirements are then incorporated into the overall information collection plan, which focuses all collection efforts, including biometric collection. Rules for processing and exploiting biometric data are developed and updated during planning and direction. Specific BEI production requirements are also identified during planning, as well as standards and guidance for disseminating and integrating BEI into future intelligence requirements or plans.

This page intentionally left blank.

Chapter 4
Collect (U)

(U) The biometric collection activity begins with validated information requirements that are answered by capturing biometric samples and their related contextual data. To meet commanders' intelligence requirements, analysts consider how biometrics are collected in all environments.

SECTION I – BEI AND INFORMATION COLLECTION (U)

4-1. (U) Knowledge is the precursor to effective action in the informational or physical domains. Knowledge about an operational environment requires aggressive and continuous operations to acquire information. Information collected from multiple sources and analyzed becomes intelligence that provides answers to the commander's critical information requirements. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). The staff ensures information collection activities support the commander's requirements by synchronizing and integrating all components of information collection. (See FM 3-55 for doctrine on information collection.)

4-2. (U) Units incorporate biometric collection requirements into the information collection plan. Units also integrate biometric collection requirements into standard operating procedures and specific actions on the objective. Biometric collection includes individual biometric samples, associated data, behavioral characteristics, and contextual data. The information collection plan should include details about how to handle captured materials if present.

4-3. (U) Actions on the objective include all actions taken after movement to the objective. The unit commander determines actions on the objective during planning. (See FM 3-21.10 for more details on actions on the objective.)

4-4. (U) Army forces conduct four tasks when executing the information collection plan: reconnaissance (See FM 3-90-2), surveillance (see FM 3-55), security operations (see FM 3-90-2), and intelligence operations (see FM 2-0). Biometrics and BEI contribute to development and continual assessment of the information collection plan. Intelligence staffs consider biometric information and BEI throughout information collection to ensure a complete all-source intelligence picture.

4-5. (U) The intelligence staff includes requirements for biometric collection in planning requirements and assessing collection. A focused biometric collection effort aids in identifying networks—both familial and organizational. The use of biometric information assists analysts in identifying individuals who may be linked to an event through forensic collections of a latent fingerprint or DNA. Collectors should adhere to the principle of collecting 10 fingerprints, two iris images, and one facial image (often called the 10-2-1 standard) as the enrollment standard because the latent print associating an individual to an event may be a small area on a finger. DNA data assists in determining familial relationships. Identity data derived from biometrics, forensics, and DOMEX are analyzed to develop products such as link diagrams and targeting packages that allow for precise targeting and development of named areas of interest. (Table 4-1 on page 4-2 illustrates biometric-related tasks performed during planning requirements and assessing collection.) (See ATP 2-33.4 for network analysis techniques.)

Table 4-1. (U) Biometric-related tasks during planning requirements and assessing collection

Commander's input
• Visualization. • Situational awareness. • Situational understanding. • Approval of the commander's critical information requirements, including those BEI can contribute to answering. • Intent.
Staff input
• Prepares and updates running estimates. • Evaluates organic biometric assets for— ▪ Availability. ▪ Capability. ▪ Sustainability. ▪ Vulnerability. • Develops requests for information. • Develops requirements.
Requirements development—intelligence staff
• Consolidates and validates biometric requirements. • Recommends appropriate biometric taskings for organic assets to the operations staff. • Submits biometric requests for information to higher and lateral commands. • Obtains current biometrically enabled watch list from higher.
Planning requirements tools development—intelligence staff
• Develops a requirements matrix. • Develops biometric indicators. • Develops specific information requirements. • Develops an information collection matrix. • Develops a collection synchronization matrix. • Develops and disseminates the relevant biometrically enabled watch list for the area of operations.
Execution of tactical tasks assessment—entire staff
• Monitors the tactical situation. • Maintains synchronization with operations. • Screens reporting to ensure task completion. • Correlates report to requirements. • Provides feedback to assets. • Cues assets collection opportunities. • Recommends retasking of assets. • Collects biometrics in accordance with the 10-2-1 standard and commander's intent. • Inserts biometric collections into appropriate systems.
Planning requirements tools update—intelligence staff
• Receives inputs from the commander and staff. • Eliminates satisfied requirements. • Develops and adds new requirements. • Transitions to the next operation. • Assesses biometric collections for follow-on operations.
UNCLASSIFIED

4-6. (U) Planning requirements effectively focuses information collection activities on obtaining the information commanders and staffs require to influence decisions and operations. These information collection activities include—

- Commander and staff efforts to synchronize and integrate information collection tasks throughout the operations process.
- Commander's understanding and visualization of the operation by identifying information gaps, aligning assets and resources against the gaps, and assessing the collected information and intelligence to inform the commander's decisions.
- Staff's integration processes during planning, preparation, and execution (for example, IPB, the MDMP, and the targeting, operations, and intelligence processes).

4-7. (U) Information collection synchronization integrates the intelligence product with reconnaissance and surveillance tasking. Tasking for biometrics includes specific guidance to collectors to enroll all persons of interest. Time constraints and time on target vary with each mission, but a detailed prioritization for performing these biometric tasks allow Soldiers to organize and execute accordingly.

4-8. (U) Biometric information answers information requirements such as confirmation or denial of an enemy's identity. It also provides targeting information. Biometric enrollments answer the *who*, *where*, and *when*, of persons of interest during an operation. The *what* and *why* intelligence questions are answered when biometric information is incorporated into planning. Effective operations are better synchronized with subordinate and higher echelons throughout the biometric enterprise by using the information collection plan to facilitate biometric collection efforts. (See ATP 2-01 for planning requirements and assessing collection techniques.)

COLLECTION ACTIVITIES (U)

(b) (3)

4-10. (U) Every operation potentially provides the opportunity to collect biometric information. Quality biometric collections are desired over quantity. High-quality enrollments contained in the database increase the probability that a person of interest will be properly identified. Tactical leaders should consider the following:

- As operator proficiency with biometric equipment improves, the quality of collections increases, thus speeding production.
- Preexecution checks` are essential to biometric collection success and include—
  - Equipment function checks.
  - Current BEWL loaded. (See paragraphs 5-31 through 5-39 for information on BEWLs.)
  - Adequate power or charge.

- Biometric data should be collected at every opportunity to the 10-2-1 standard enrollment. Factors limiting biometric collection include number of collection devices, area security, and subject bodily disfigurements (such as, amputations, burns, scars).
- Postmission checks include uploading biometric data into theater- and national-level databases.

4-11. (U) Collecting and handling biometric data is challenging, depending on the environment, cooperation of the subject, time available, equipment, and other factors. DOD and other U.S. Government agencies and organizations recognize specific standards for collection, handling, and dissemination of biometric and contextual data. (See the *Electronic Biometric Transmission Specification* [also called EBTS].) All Army collection systems and databases are required to meet these standards so the entire intelligence community can benefit from shared biometrics and forensics data.

4-12. (U) A full (also called standard) biometric enrollment consists of a facial image, iris images, and fingerprints. However, each biometric modality has a distinct set of advantages and disadvantages when compared to others. Mission dictates which modalities are collected. Other factors, such as time on objective or collection assets available, also affect what can be collected. Joint force and command guidance commonly outline the collection expectations. However, if the mission and situation allow, a full biometric enrollment is accomplished. (See appendix B for more advantages and disadvantages of different modalities.)

4-13. (U) Most biometric collection systems accommodate collection of multiple biometric modalities on the same system (multimodal capability). Multiple biometric modalities are collected during an enrollment event. This allows a more complete collection file of an individual, thus increasing efficiency of comparisons and accuracy of results.

CULTURAL IMPACT OF COLLECTIONS (U)

4-14. (U) Cultural considerations and impacts from biometric collections include—

- Not all cultures understand what biometrics are and why it is necessary to collect them.
- Some cultures may be suspicious or superstitious about collections.
- Certain cultures may feel violated by collections.

4-15. (U) Mission accomplishment relies on cross-cultural communication and engagement and military information support operations during biometric collections to mitigate any cultural misunderstanding.

4-16. (U) The limits of biometric and forensic effectiveness for legal matters may hinge on the local culture of the area in which operations are being conducted. This is particularly important for counterinsurgency and stability missions. There may be U.S.-imposed limitations on using forensic evidence because of classification levels. Host-nation rules of evidence may apply. Local judges may reject biometric and forensic evidence and, instead, require two witnesses and photographs. However, using biometrics and forensics in intelligence is valuable, especially since few, if any, of the evidentiary rules that pertain to law enforcement apply to intelligence.

CURRENT COLLECTION AND DATABASE CAPABILITIES (U)

~~4-17. (FOUO)~~ Over the last decade, in support of specific theaters of operations, DOD has developed and employed several biometric databases and capabilities. DOD biometric and forensic capabilities continue to evolve as needed to support operational needs. At present, DOD employs or has access to the current capabilities:

- Department of Defense Automated Biometric Identification System (ABIS).
- (b) (3)
- Biometric Identity Intelligence Resource (BI2R).
- Biometrics Automated Toolset–Army (BAT-A).
- Secure Electronic Enrollment Kit II (also called SEEK II).
- Defense Biometric Identification System.

AUTOMATED BIOMETRICS IDENTIFICATION SYSTEM (U)

~~4-18. (FOUO)~~ ABIS is the central, authoritative, multimodal biometric data repository. The system operates and enhances associated search and retrieval services.

(b) (3)

Note. (U) ABIS is the authoritative repository for biometric samples. Authoritative should not be construed as perfect—ABIS does report false positives. Local nonauthoritative databases in tactical collection devices are sometimes more stable and report more accurate results.

NEXT GENERATION IDENTIFICATION (U)

4-20. (U) Next Generation Identification is a large-scale 10-fingerprint (open-set) identification system. It is used for criminal history background checks and identification of latent prints discovered at crime scenes. Next Generation Identification is an FBI system managed by the Department of Justice. It is incrementally replacing the Integrated Automated Fingerprint Identification System.

BIOMETRIC IDENTITY INTELLIGENCE RESOURCE (U)

4-21. (U) BI2R is an automated database that stores biometric and associated data from DOD collection devices. Analysts use the BI2R toolset to perform analysis and develop intelligence reports supporting DOD and national missions. The system is designed to provide DOD and the intelligence community with authoritative, biometrically base-lined identities. It provides the advanced tools and technologies necessary to analyze, collaborate, produce, disseminate, and share biometric information. BI2R also interfaces with systems supporting controlled access to BI2R products via JWICS and SIPRNET.

BIOMETRICS AUTOMATED TOOLSET–ARMY (U)

4-22. (U) BAT-A is a multimodal, tactical, biometric system that collects, stores, matches, and shares fingerprints, iris images, and facial images. The BAT-A contains two important components the analyst should be aware of: the laptop system, which enables access to the BAT-A software, and the tactical handheld biometric collection device.

4-23. (U) Enrollers collect biometric, biographical, and behavioral data on persons classified as friendly, neutral or unknown, or adversary. During biometric collection, BAT-A establishes new files or matches collected data against either existing local files or other servers in the BAT-A architecture. Soldiers use the data during enrollment for identification or for verification and authentication purposes.

4-24. (U) The BAT-A system allows the digital file created on an individual to be updated. Analysts often use it to attach interrogation reports and other key data to a biometric file. Files stored on BAT-A servers are replicated in the continental United States BAT-A hub via the SIPRNET. Data from the continental United States BAT-A hub is processed through an automated cross-domain system to ensure only unclassified data is entered into ABIS. The BAT-A system represents an encounter-based system. That means one identity is updated on each encounter, when at all possible.

SECURE ELECTRONIC ENROLLMENT KIT II (U)

4-25. (U) The Secure Electronic Enrollment Kit II is 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.

DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (U)

~~4-26. (FOUO)~~ The Defense Biometric Identification System is a DOD-owned and -operated system developed by the Defense Manpower Data Center as a force protection program to manage installation access control for military installations. (b) (3)

(b) (3)

EXPLOITATION OF CAPTURED MATERIALS (U)

4-27. (U) Modern military operations are executed in complex and ever changing operational environments. Military leaders at all levels must have access to accurate and timely information. Leaders' decisions are enabled by accurate information about enemy forces through rapid extraction, exploitation, and analysis of captured materials. Captured materials are divided into captured enemy documents and media and captured enemy materiel.

4-28. (U) Captured materials and residual collection, such as latent prints, are a fertile source of biometric data. Exploiting captured materiel has long been practiced in the Army as technical intelligence (TECHINT). *Technical intelligence* is intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0). TECHINT applies scientific and technical methods to fulfill national security, counterterrorism, and counterinsurgency requirements. (See ATP 2-22.4 for TECHINT techniques.)

4-29. (U) *Document and media exploitation* is the processing, translation, analysis, and dissemination of collected hardcopy documents and electronic media that are under the U.S. Government's physical control and are not publicly available (ATP 2-91.8). DOMEX includes the systematic extraction of information from all media in response to commanders' collection requirements. When conducted properly, DOMEX—

- Maximizes the value of information obtained from captured enemy documents and media.
- Provides the commander with timely, accurate, and relevant intelligence to effectively enhance awareness of the threat's capabilities, operational structures, and intents.
- Assists in criminal prosecution and legal proceedings by maintaining chain of custody procedures and preserving the evidentiary value of captured enemy documents and media.
- Allows for strategic and long-term analysis within the intelligence and law enforcement communities.

4-30. (U) DOMEX is an increasingly specialized, full-time mission that requires advanced automation, communications, and analytical support, as well as expert linguists. DOMEX consists of three components—document exploitation, media exploitation, and cell phone exploitation. (See ATP 2-91.8 for DOMEX techniques.)

4-31. (U) DOMEX complements TECHINT. Both support—

- Intelligence production.
- Targeting.
- Interrogation operations.
- Warning intelligence for protection.
- Criminal prosecutions and judicial proceedings.
- The collection of biometrics and forensics.

4-32. (U) DOMEX and TECHINT provide significant intelligence, but neither has the certainty of source provided by biometrics. By understanding and employing aspects of DOMEX and TECHINT, analysts can better exploit and integrate forensics and FEI into the overall BEI intelligence picture.

SECTION II – FORENSIC-ENABLED INTELLIGENCE (U)

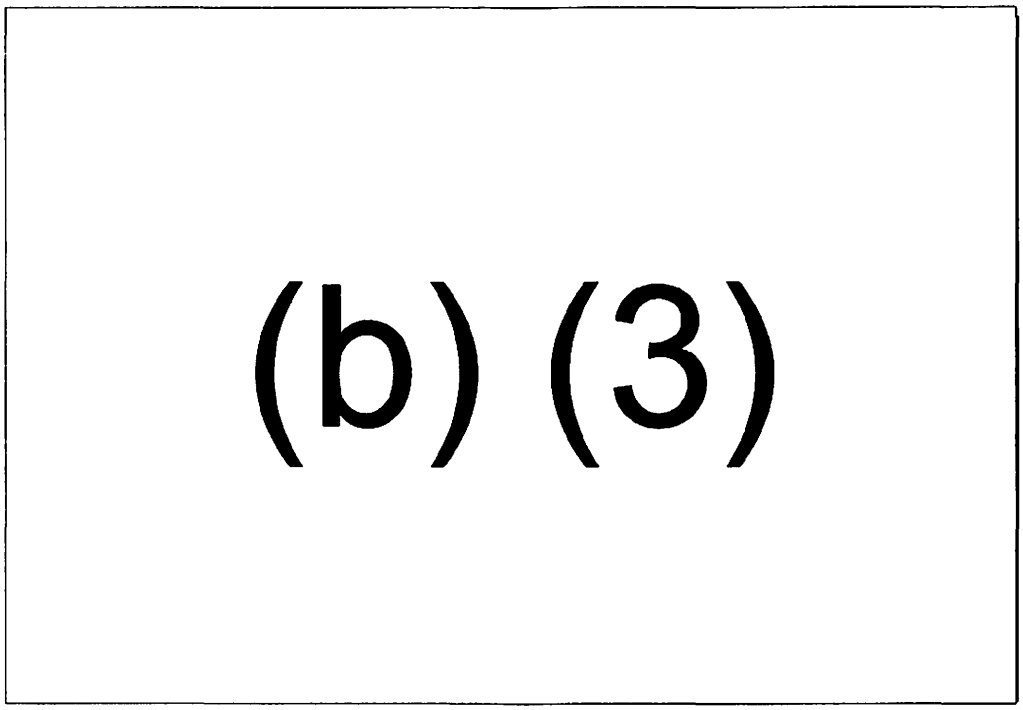
4-33. (U) BEI and FEI contribute to minimizing anonymity and positively identifying individuals in both military operations and national-interest-related business functions. Forensics involves the scientific analysis of linking persons, places, things and events.

4-34. (U) *Forensic-enabled intelligence* is the intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest (JP 2-0). It is the result of the evaluation, analysis, and synthesis of forensic data. FEI can provide the ability to identify and characterize possible persons of interest and materiel and link them to organizations, places, things, intentions, and activities. FEI offers critical information supporting commanders and decisionmakers by advancing situational awareness and understanding of the area of operations. Additionally, FEI supports joint staff and force protection concepts by providing information that enables intelligence, targeting, prosecution, personnel recovery, medical, component materiel sourcing and other warfighting functions throughout the range of military operations.

4-35. (U) Forensic collection includes, but is not limited to, latent fingerprints and DNA. Such collection can occur during site exploitation activities by properly trained personnel. FEI has a large impact on intelligence operations and, more specifically, BEI by linking individuals to specific events, organizations, or military threats. FEI is used most extensively during combat operations to support intelligence development as opposed to being used for legal or prosecutorial matters.

Forensic-Enabled Intelligence Support to Intelligence (U)

(b) (3)



Chapter 5
Produce (U)

(U) Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format. (See ADRP 2-0.) Biometrics and BEI are critical elements of all-source intelligence that lead to more comprehensive intelligence products and a better understanding of the operational environment.

PROCESSING, EXPLOITATION, AND DISSEMINATION (U)

5-1. (U) At the most basic level, the intelligence warfighting function observes things about the threat and relevant aspects of the operational environment and collects data that is processed and exploited into usable information for analysis and production, which results in intelligence. Army doctrine has long recognized the functions of processing, initial analysis, and reporting, as well as the requirement for providing combat information. However today, processing, exploitation, and dissemination (PED) requirements have grown significantly. There are many different capabilities that support it.

5-2. (U) PED refers to the execution of the related functions that convert and refine collected data into usable information, distribute the information for further analysis, and provide combat information to commanders and staffs. In essence, PED is the way that the intelligence warfighting function processes collected data, performs some initial analysis (exploitation), and provides information in a useable form for further analysis. While performing these functions, some of the information will meet the criteria of combat information. In those cases, the combat information is disseminated to commanders and staffs per unit standard operating procedures. An important part of PED is ensuring that the information is distributed with adequate context and is formatted to make subsequent analysis easier or to facilitate a better understanding of the combat information. Another important aspect of PED is providing feedback on the effectiveness of the collection relative to the tasking and expected results.

5-3. (U) The Army's current approach to PED reflects a much more deliberate solution to the complexity of intelligence operations and the explosion of available data and information that results from information collection. In the future, the amount of available data and information will continue to grow exponentially. The Army's new approach to PED includes both a far greater emphasis on resourcing, planning, executing, and maintaining a continuous assessment of PED. This approach to PED is accomplished through various PED capabilities.

5-4. (U) PED capabilities are the personnel, specialized intelligence and communications systems, and software and advanced technologies that execute PED. Other resources are often required to allow PED capabilities to operate, including bandwidth, databases, and network architecture. PED capabilities can be organic to the intelligence unit, task-organized, or distributed from a centralized location through the network as required.

5-5. (U) Commanders and staffs resource and prioritize supporting and distributed intelligence capabilities, to include PED capabilities, through thorough staff planning. The ways these capabilities communicate and interoperate are accounted for in the intelligence architecture. Within the intelligence architecture, PED capabilities are functionally and technically linked to the intelligence communications networks, data and information repositories, and the military intelligence organizational backbone

(sometimes referred to as the foundation layer of the intelligence enterprise). Executing effective biometric activities requires resourcing, planning, and preparing the use of specific biometric PED capabilities.

BIOMETRIC PRODUCT CATEGORIES (U)

5-6. (U) Biometric data obtained to meet an intelligence collection requirement results in classified data in some cases, due to the sources and methods used to obtain them. Classified collection operations have significant effects on the design of the supporting architecture—chiefly in the match and store functions. Classified biometric samples should never be matched or stored in unclassified databases. A subsequent match of an unclassified sample to a classified sample within the database could threaten to reveal the sources and methods by which the classified sample was obtained. (See chapter 7 for detailed information on match and store functions.)

5-7. (U) One of the most important elements of exploiting BEI is alerting the original collector to enrollments that result in high-profile biometric matches (for example, those previously discovered by forensics exploitation teams at IED sites). Analysts receive match reports after each subsequent enrollment of an individual's biometric information into ABIS. An enrollment with a confirmed forensic match of latent prints at an IED explosion site can prove very important. This BEI feedback enables commanders to make better operational decisions based on current operational conditions and highlights the importance of collectors adhering to enrollment standards that ensure good biometric collections.

5-8. (U) BEI products are characterized in terms of timeliness. The three categories of products are immediate, current and strategic.

IMMEDIATE BEI PRODUCTS (U)

5-9. (U) Immediate BEI products result from biometric data collected at the point of encounter and compared to previously created biometric files stored in the local database. Products support the commander's decisionmaking in real time—for example, a decision whether to detain or not detain. The match is limited by the local database information on when, where, and under what circumstances the individual was encountered.

CURRENT BEI PRODUCTS (U)

5-10. (U) Current BEI products are not as timely as immediate products. Analysts use current products to combine contextual data with other all-source information. The reports are distributed and match reports are analyzed before uploading into BI2R. Results produce current intelligence products, such as a biometric identification analysis report (BIAR). These are entered into the BI2R and are appended to the individual's biometrically linked identity intelligence profile (BLIIP).

STRATEGIC BEI PRODUCTS (U)

5-11. (U) Strategic BEI products can be developed in any format and generated at all echelons. Strategic products are typically long-term studies but can be completed within a shorter period, depending on the requirements. BLIIPs are combined with products of other intelligence disciplines to support broader analytical products including, but not limited to, network analysis, geospatial analysis, IPB, named areas of interest, and density plot overlays.

PROCESSING BIOMETRIC MODALITIES (U)

5-12. (U) Biometric samples obtained from a live enrollment using a tactical handheld biometric collection device can be compared and matched against samples stored in a database or against the BEWL. This match allows the collector to make an immediate decision based on the commander's guidance and established standard operating procedures. To be considered fully exploited, the collected biometric data must continue through the entire biometric process and all-source analysis. (See appendix B for more information about modalities. See paragraphs 5-31 through 5-39 for information on BEWLs.)

FINGERPRINTS AND DNA (U)

5-13. (U) Site exploitation can involve collecting latent biometric samples. A *latent sample*, most frequently a fingerprint, is dormant, inactive, or nonevident biometric residue that is collected, measured, and stored. Latent biometric samples are those that are left behind on materiel or surfaces. Once the latent biometric samples are collected, they are processed and compared. The comparison may occur at multiple levels, from tactical to national.

5-14. (U) In the case of latent fingerprints and latent DNA, the samples are collected and formatted in a tactical setting. These samples are processed and catalogued at the joint force regional forensic center or at an equivalent expeditionary forensic laboratory.

5-15. (b) (3)

5-16. (FOUO) DNA collections fall into one of three categories: questioned, unknown, or referenced sample from a live, known individual. Samples are first processed by a forensic lab, such as the Defense Forensic Science Center or the Armed Forces DNA Identification Laboratory. The resulting DNA profiles are then compared and stored in DNA databases at those locations. Comparison results, such as matching or DNA associations, are generated and disseminated to the submitting agency for use in exploitation, analysis, and intelligence production.

FACIAL IMAGES (U)

5-17. (b) (3)

IRIS IMAGES (U)

5-18. (b) (3)

COMPARISON (U)

5-19. (U) Comparison begins with receipt of the collected, standardized biometric file—the recognition biometric sample. The comparison activity is commonly referred to as the "match" or "matching" action. The comparison process involves comparing a biometric reference with a previously stored reference, or references, in order to identify or verify the identity of a person.

5-20. (b) (3)

5-21.

5-22.

5-23. (b) (3)

POSTCOMPARISON PROCESSING (U)

5-24. (b) (3)

MATCH MANAGEMENT AND BIOMETRIC WARNING INTELLIGENCE (U)

5-25. (b) (3)

5-26.

5-27. (b) (3)

5-28. (b) (3)

BEI PRODUCTS (U)

5-29. (U) BEI products are used increasingly to support Army operations. The following BEI products are currently in use at all levels. Many of these biometric products are requested from the National Ground Intelligence Center or Defense Intelligence Agency. BEI products support analysts during IPB, the MDMP, and targeting. As the field of biometrics and BEI matures, these product types may change or be eliminated as needed.

BIOMETRIC ANALYSIS PACKAGE (U)

5-30. (U) The biometric analysis package serves as a detailed analysis on a particular individual or event of interest. It provides a geospatial depiction of all known locations for the subject and the subject's associates. A package highlights biometric links among individuals operating within the subject's territory. It also lists other watch-listed individuals whom the subject may have known or have information about, based on the proximity of enrollments. Primarily used for operational planning, this product can include biometric named areas of interest specifically tailored to the purpose of encountering the individual. (See paragraphs 7-33 and 7-34 for details on the biometric named area of interest.)

BIOMETRICALLY ENABLED WATCH LIST (U)

5-31. (U) A *biometrically enabled watch list* is any list of persons of interest with individuals identified by biometric sample or the sample's unique identification number instead of by name, and the desired or recommended disposition instructions for each individual. BEWLs are used for screening purposes. The identification number, or biometric reference number, is the unique number assigned by an authoritative database. Examples of identification numbers are the transaction control number that ABIS assigns to each biometric sample and the global unique identifier assigned to each biometric file in BAT-A.

5-32. (U) Biometric support to developing watch lists is similar to intelligence support to target development. (See ADRP 2-0 and FM 7-15.) BEI is incorporated into all-source analysis of potential persons of interest, resulting in a documented and validated nomination of a person of interest to a tactical, operational, DOD, or national-level watch list for identification, screening, locating, tracking, or interdiction purposes.

5-33. (U) The DOD BEWL is a decision aid to help commanders determine what action to take when encountering a person of interest. In some areas of responsibility and theaters of operations, the DOD BEWL provides basic recommendations for each person of interest encountered. Persons of interest are assigned to a tier on the DOD BEWL. Each tier has recommended actions associated with it. Examples of recommendations include detain, deny training or benefits, deny access to U.S. facilities, and track or assess. (See appendix C for an example of guidance associated with BEWL tiers.) The track or assess recommendation is an analytic trigger that alerts the relevant intelligence staff that a person encountered may be a person of interest.

5-34. (U) A BEWL itself is different from the reference databases that house the biometric files of the individuals on the BEWL. For example, the DOD BEWL currently uses three reference biometric databases: ABIS, BAT-A, and the Department of Homeland Security Automated Biometric Identification System (IDENT). Each of these databases contains a different set of files that the DOD BEWL draws from. (See appendix C for examples and more information about watch list tiers and categories.)

DOD Biometrically Enabled Watch List Interfaces (U)

5-35. (U) The DOD BEWL is maintained within BI2R by the Identity Intelligence Division of the National Ground Intelligence Center. Biometric samples of individuals on the DOD BEWL generate an automatic alert within ABIS, BAT-A, Next Generation Identification, IDENT, and biometric matching systems within the governments of select foreign partners.

Unit Responsibilities (U)

5-36. (U) The fields and tiers within a BEWL are tailored to applicable areas of operations. This structure is also tailored to mission requirements by each geographic combatant command. Each unit should assign a BEWL manager from the intelligence staff, including the company intelligence support team (COIST) at the company level, in order to maintain an accurate BEWL registry. BEWL manager duties include—

- Developing an operational watch list structure, within the limits of the local governing rules of engagement or security agreements, that corresponds with the DOD BEWL's basic actionable categories of detain, deny, or track. (A watch list structure may include such details as tiers, recommendations, and standard operating procedures.)
- Developing and maintaining a watch list that encompasses subordinate units' watch lists.
- Assuring that persons of interest included on the watch list have at least one collected biometric sample.
- Coordinating any nominations for the watch list with the next higher command on a regular schedule.

Managing the Biometrics-Enabled Watch List at Each Echelon (U)

5-37. (U) BI2R's ability to create specialized subsets of BEWL files allows combatant command and joint task force intelligence staffs to manage unit and regional BEWLs based on criteria that meet host-nation agreements and the local commander's intent.

Nomination and Removal Procedure (U)

5-38. (U) Any intelligence community organization or combatant command can nominate an individual for addition to or removal from the BEWL. BEWL managers need to review regularly the tier or level and alert status of the persons of interest within their area of operations. Prior to nominating an individual to the watch list, the nominating unit determines whether the individual meets the prerequisites for inclusion on the watch list and recommends the appropriate tier to higher headquarters or appropriate BEWL manager. Tiers are tailored according to combatant command, joint force, and Defense Intelligence Agency guidance. When appropriate, the National Ground Intelligence Center nominates persons of interest to the national watch list programs through the Defense Intelligence Agency. Agencies consider the following when making nominations:

- The final criteria for inclusion, taking into account applicable agreements and host-nation laws.
- At a minimum, nominations must have a collected biometric sample.
- The nominated biometric sample must be marked as designated by ABIS to facilitate the sample's placement in the ABIS database.
- Nominations must meet the justifiable criteria for the specific tier to which the individual is nominated.
- Nomination of U.S. persons must be handled in accordance with AR 381-10.

5-39. (U) Units establish procedures for removing individuals from the watch list or downgrading the tier they are assigned to. These actions are triggered by a change in an individual's threat level, status, or the rules of engagement. Normally, individuals removed from tiers one (detail) or two (question) meet the criteria for placement on tier four (deny access). Individuals removed from tier three (assess) may be placed at other tiers or removed from the watch list completely. However, procedures should address when to coordinate with the appropriate intelligence analyst regarding a tier three individual. Prior to changing an individual's status, the unit determines whether the individual meets the prerequisites for the new tier, using established criteria. The unit then recommends to higher headquarters the appropriate tier or complete removal. (See appendix C for more information on tiers.)

BIOMETRIC-FOCUSED AREA STUDY (U)

5-40. (U) The biometric-focused area study is a detailed research document that focuses on a specific area (such as a village, district, or province) or a specified route. The product is designed to assist in operational planning and increase the unit's knowledge of the type of threat individuals in the area and of the indigenous population. A study displays the following:

- Biometric enrollments of individuals on the BEWL, with accompanying biographical data.
- Density plots of forensically exploited captured enemy documents, media, and materiel.
- Individuals who have matched to cases of interest.
- A biometric network analysis chart highlighting individuals who are biometrically associated to the same evidence.

BIOMETRIC INTELLIGENCE ANALYSIS REPORT (U)

5-41. (U) A BIAR is an intelligence product that associates a match with an individual in the biometric database. It is produced by sorting, analyzing, and linking the match, the individual's history, and related information and intelligence. A BIAR contains the identification, background, and assessment of the intelligence value of the subject. The report is produced for all high-value latent matches, other high-threat matches, and matches from specified areas. BIARs may be requested directly from the National Ground Intelligence Center. (Figure 5-1 on page 5-8 depicts an example of a training BIAR.)

BIOMETRICALLY LINKED IDENTITY INTELLIGENCE PROFILE (U)

5-42. (U) A BLIIP is a card view of a search result. It contains links to all other files with the same biometric identification. An individual may have multiple BLIIPs, one for each encounter. A photograph of the individual is located on the profile, and the color of the surrounding box is a visual indicator of the individual's alert status. (Figure 5-2 on page 5-9 displays a training example of a BLIIP.)

BIOMETRIC PLACEMENT AND ACCESS PACKAGE (U)

5-43. (U) The biometric placement and access package is a product based on the successful law enforcement line-up principle. Human intelligence (HUMINT) collectors use the line-up as one tool for assessing a particular source's knowledge of other persons of interest and their involvement in known networks. The line-up can also assist in vetting by helping determine if the source in question is providing false information.

5-44. (U) A biometric placement and access package displays photographs and biographical data of known associates of an individual or individuals of interest who may operate in the same area as the subject in question. Photographs of known associates to a particular person of interest are seeded with random photographs of individuals not associated with that person. The source is then asked to pick the person of interest or people associated with that person out of the line-up.

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(3) 50 USC §3024(i)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

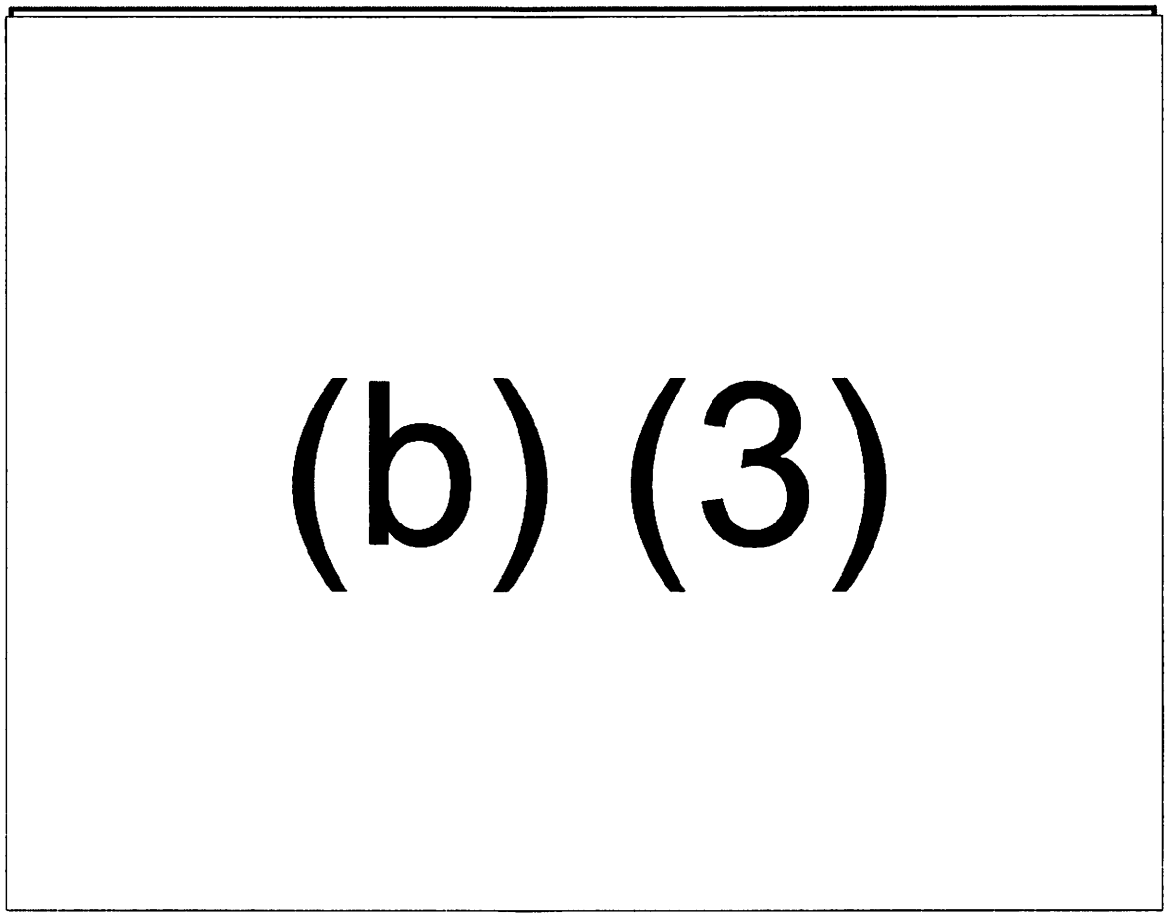
☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 48

IAGPA-CSF Form 6-R
1 Sep 93



HUMAN INTELLIGENCE SUPPORT PACKAGE (U)

5-45. (U) A HUMINT support package is a biometrically derived, geospatially referenced product developed using a series of data mining and refinement processes. This product is designed to aid HUMINT collectors in the spotting and assessing phase of source development. The leveraged resources include, but are not limited to—

- DOMEX.
- First- and second-order associations.
- Residence.
- Employment history.
- Pattern of life analysis.
- Familial relations.
- Travel.

Note. (U) All information pertaining to HUMINT sources must be closely guarded from widespread dissemination and maintained within 2X (human intelligence and counterintelligence) staff channels.

BIOMETRIC TARGET INTELLIGENCE PACKAGE (U)

5-46. (U) The biometric target intelligence package (also called a tracking intelligence package) is an intelligence product created by biometric analysts for a single person of interest. It is a consolidated product that captures the related intelligence about the individual in a one- to two-page presentation slide format. A package includes relevant data on the individual's known biometrics, associated data, and circumstances of the most recent encounter. The product may include a map with locations relevant to the person of interest,

as well as a network chart to portray connections. Additionally, the package may also include embedded files, such as separate serialized reporting, open-source data, or the individual's raw biometric data.

CRIMINAL ACTIVITY ANALYSIS REPORT (U)

5-47. (U) The criminal activity analysis report is unclassified and prepared in a storyboard format. It may be approved for release to multinational partners and host-nation forces by a foreign disclosure officer. This report is used to aid in the detention of individuals biometrically associated with captured enemy documents, media, or materiel. It is also used to support prosecution in a host-nation court. A report is routinely requested when apprehension of a known individual is matched to evidence associated with criminal activity. It includes—

- Biological characteristics and associated data on the matched individual.
- Generic case information, to include—
  - Casualties.
  - Location of the evidence recovery.
  - Evidence overviews, with graphics.
  - A biometric link analysis diagram.
  - A summary of the individual's criminal activity.

NETWORK ANALYSIS OF BIOMETRIC MATCHES (U)

5-48. (U) A network analysis of biometric matches concentrates solely on biometric cases within a specific area and the individuals biometrically associated with those cases. This product is composed of a network analysis chart that displays the connections among various individuals through biometric matches to evidence and detailed descriptions of individuals of interest.

PROSECUTION SUPPORT PACKAGE (U)

5-49. (U) A prosecution support package is an unclassified packet used to support prosecution in a host-nation court. It is requested after an individual has been detained after being biometrically associated with captured enemy documents, media, or materiel. The prosecution support package includes biological and biographical data on the matched individual and detailed case information. This includes detailed information showing the relation between the individual's known biometrics and exploited forensics as well as—

- Damage or casualties that resulted from the incidents.
- Location of the evidence recovery.
- Evidence overviews with graphics.

WARRANT SUPPORT PACKAGES (U)

5-50. (U) Warrant support packages are sets of documents that assist in obtaining criminal arrest warrants. These packages are prepared to assist host-nation law enforcement personnel and judicial bodies and are admissible in court.

5-51. (U) Although not a pure biometrics-enabled product, the warrant support package is supported by BEI and contains releasable data from an event or series of events biometrically linked to an individual. The information contained in a warrant support package includes a timeline and data about each of the linked biometric collection events. The collection events can include data of all modalities, including fingerprints, DNA, and unknown latent fingerprints recovered from collected materials. The final piece of the warrant support package exhibits the results of the examination and identification determined by the biometric collection devices. Warrant support packages are submitted to a nonintelligence, court-recognized subject matter expert, who testifies concerning the information included in the package. Once a package is accepted, an arrest warrant is signed and served.

Chapter 6
Disseminate (U)

(U) Commanders must receive combat information and intelligence products in enough time and in an appropriate format to facilitate situational understanding and support decisionmaking. BEI products that are disseminated include biometric files, comparison results, encounter-tracking reports, alerts, transaction data, enterprise metrics, and BEI data and products to appropriate personnel.

BIOMETRIC ENTERPRISE ARCHITECTURE (U)

6-1. (U) Biometric files are shared through DOD-approved biometric data exchange portals and other sharing systems. DOD, interagency, and multinational partners share files as mutually agreed upon or otherwise allowed by law and policy. Biometric sharing agreements with partner nations may have caveats as to how, when and with whom biometric data may be shared. Commanders should obtain appropriate-level legal review before sharing biometric files or match results to ensure compliance with law, policy, and foreign agreements.

6-2. (U) The DOD biometric enterprise architecture transmits files using various networks and across various domains. These networks and domains can change or be updated as necessary to support specific current operations or capability needs. The architecture provides fast, continuous global communications to all echelons. It gives Army forces an identification and verification capability. In addition, it further enables cross-functional analysis with information derived from intelligence disciplines such as signals intelligence and HUMINT. A biometric system, with its supporting automation, directly or indirectly is an intelligence information collection and processing capability that provides information to analysts.

6-3. (b) (3)

Note. (U) Intelligence databases are subject to intelligence oversight and the Privacy Act of 1974 with regard to any U.S. person information they may contain. EO 12333, DOD 5240.1-R, and AR 381-10 govern the collection, retention, and dissemination of information on U.S. persons. If information on U.S. persons is encountered, such information must be annotated in the fields provided in the biometric enrollment system so intelligence analysts can handle the data properly pursuant to intelligence oversight handling requirements.

6-4. (U) Due to classification and need-to-know limitations, not all interested parties have access to complete biometric files and BEI products. Some databases may require the analyst to request a username and password. The output of the BEI process frequently includes recommendations for commanders and Soldiers. BEI analysis can influence, but not direct, decisionmakers and commanders.

6-5. (b) (3)

BIOMETRIC DATA FLOW (U)

6-6. (U) Figure 6-1 depicts the biometric data flow as it occurs from the tactical level of operations through the strategic level, across different systems and domains. The figure illustrates the data flow from single collection capabilities through tactical biometric collection points, to processing and analysis activities, and the return of results to customers at all levels. It includes classified and unclassified biometric information.

6-7. (b) (3)

(b) (3)

DATA ROUTING (U)

6-8. (b) (3)

(b) (3)

DATA SHARING (U)

6-9. (b) (3)

(b) (3)

6-10. (b) (3)

(b) (3)

6-11. (U) Analysts must understand their unit's capabilities and limitations when disseminating biometric information. Typically, a unit is issued biometric collection devices according to its table of organization and equipment. Intelligence staffs update the devices with the most recent BEWL and extract new data when necessary. However, most non-military-intelligence personnel do not have access to U.S. Government biometric databases. Echelon intelligence officers must develop alternative methods to disseminate critical, time-sensitive biometric information to the right personnel, at the right time, and in a useable format. (This task should be performed during planning and preparation for the operation.)

6-12. (b) (3)

(b) (3)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(3) 50 USC §3024(i)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 53

IAGPA-CSF Form 6-R
1 Sep 93

6-13. (U) The most important consumer of BEI is the commander. When the collection of biometrics is part of the intelligence and operational planning phases and BEI is fully integrated into the all-source intelligence picture, the commander has better situational understanding. Commanders determine how they want to receive BEI, but generally analysts provide it in written narrative, verbal narrative, or in the recommended graphic format.

Chapter 7
Analyze and Assess (U)

(U) Analysis contributes to assessing threat capabilities and vulnerabilities. Biometric collection efforts are cyclical. As part of all-source intelligence development, collected biometric data is evaluated, analyzed, and combined with other information and intelligence for a complete intelligence picture.

EVALUATING, ANALYZING, AND SYNTHESIZING BEI INTO ALL-SOURCE INTELLIGENCE (U)

7-1. (U) Successfully developing BEI requires a good grasp of the larger intelligence picture when incorporating biometric data into it. Army forces conduct operations based on all-source intelligence assessments and products developed by the echelon intelligence staffs. *All-source intelligence* is the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations (ADRP 2-0). All-source intelligence is used to develop the intelligence products necessary to aid situational understanding, support the development of plans and orders, and answer information requirements. Although all-source intelligence normally takes longer to produce, it is more reliable and less susceptible to deception than single-source intelligence. All-source analysis is continuous and occurs throughout the intelligence process.

7-2. (U) *Intelligence analysis* is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production (ADRP 2-0). This process is dynamic and continuously integrates new and existing information throughout the effort. It also ensures that all information goes through a logical, criterion-based process of determining its value prior to updating existing assessments. (See ATP 2-33.4 for additional information on intelligence analysis.) The steps of intelligence analysis are—

- **Evaluate**—when the data of reporting are assigned a value respective to the source and application of the data.
- **Analyze**—when data from information reports is dissected into each subcomponent of the report.
- **Synthesize**—when the data is combined with previous holdings to update existing products, change previously accepted assessments, corroborate existing assessments, or create new assessments.

7-3. (U) BEI is a product of biometric information, threat information, and other information relating to the operational environment. By evaluating, analyzing, and synthesizing all of these elements, the analyst can produce better BEI. Figure 7-1 on page 7-2 displays the components of intelligence and information to consider when developing BEI. The components displayed are not all-inclusive—analysts need to determine what information is relevant to their situation by understanding the commander's intent and information requirements. When biometric information is evaluated, analyzed, and synthesized with all-source intelligence within the intelligence process, it allows the intelligence staff to develop a more complete picture of the threat. BEI aids commanders in making decisions about targeting and protection by identifying individuals or verifying individual identities.

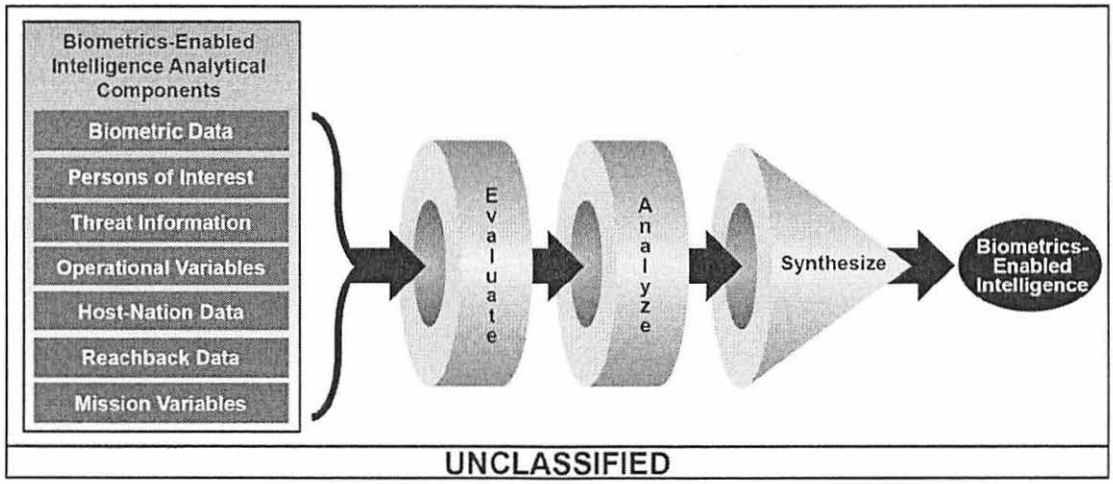


Figure 7-1. (U) Analytical components to consider when developing biometrics-enabled intelligence

7-4. (U) The BEI analytical components contribute to the development of BEI products and are integrated into the intelligence process. Biometric data is only one source of information; however, when it is combined with all-source intelligence, the analyst has a much better probability of answering identity-related questions as well as commanders' information requirements.

7-5. (U) BEI analysis can be triggered by the comparative response from either a local database or ABIS. In general, analysis begins in one of three ways:

- In response to the results of the comparison or match action.
- In response to a biometric enrollment.
- Because of a requirement to locate data for a person of interest.

7-6. (U) Biometric information adds a factual layer of data or intelligence to the analysis process by providing positive identification or verification of the identities of persons of interest. Once the biometric layer is in place, tailored overlays can provide further data and information to incorporate into the synthesis and integration efforts. Bomb-maker information, social network analysis, threat unit verification, battle damage assessment, and information received from partner nations are examples of information that are combined with the factual biometric layer to construct a tailored overlay.

7-7. (U) As collection against a target occurs, additional analytical efforts by both the intelligence and operations staffs can identify other members of the network and seek key nodes identified by biometric data. When an identification is made, the individuals composing the network are nominated for placement on a BEWL and the network itself is targeted for further collection activity.

7-8. (U) Fundamental intelligence analysis does not change because of different environments. When analysts understand the operational environment and commander's requirements, they can actively collect information, including biometrics and forensics, and analyze that information in the context of history, capabilities, current situation, and threat objectives. Analysts focus efforts on how they can employ biometric information effectively and develop it into BEI.

7-9. (U) Analysis produces intelligence that, along with staff recommendations, aids commanders in deciding whether an individual is friendly, neutral, unknown, or adversary. Categorizing persons in this manner helps commanders quickly provide enough guidance for Soldiers to make decisions and act on the information provided.

7-10. (U) Figure 7-2 displays the process that biometric data goes through when entered into a database such as ABIS. A biometric sample is entered into the database for current and future reference. Analysts

access and evaluate biometric files and their data to support intelligence activities such as situation development, support to targeting, and all-source production.

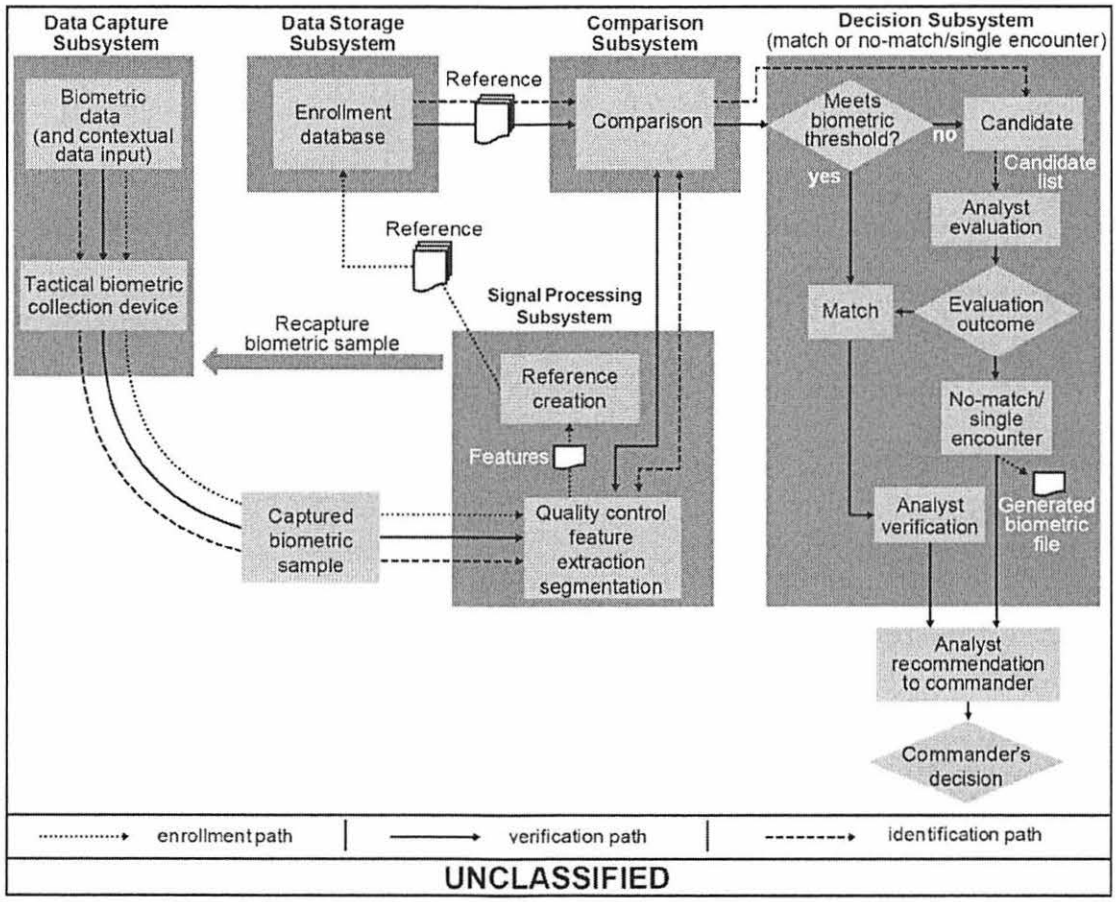


Figure 7-2. (U) Analytic processing of biometric data

BIOMETRIC ANALYSIS (U)

7-11. (U) The analyze activity draws heavily on the match and store actions of the biometric automated process. (See paragraphs 2-6 through 2-11.) The analyst's objective is to link or associate the data that has been mined from an authoritative database with data collected from a biometric enrollment. Linking occurs when associated data are connected to a biometric sample. Successful linking results in the conclusion that two or more seemingly disparate identity characteristics belong to the same person. Factors involved in biometric analysis include the following:

- The type of biometric database response to the query.
- The collection capability used.
- The type of biometric storage site queried.
- The results of biometric searched undertaken in response to a query.

BIOMETRIC DATABASE RESPONSES (U)

7-12. (U) Four types of responses can be received from the DOD authoritative database (ABIS):

- Match.
- No-match/single encounter.
- Uncertain.
- Error.

Match (U)

7-13. (U) A *match* is a comparison determination that a newly entered biometric sample or samples and the biometric reference are from the same source. The enrollments may be from various sources, such as a biometric device collection (fingerprint, iris image, or facial image), latent fingerprint collection, or inked fingerprint cards.

No-Match/Single Encounter (U)

7-14. (U) A *no-match/single encounter* is a comparison determination that a newly entered biometric sample or samples and the biometric reference are not from the same source. The biometric system creates a new biometric file containing the sample or samples. Encountering and enrolling the individual again based on a different sample will result in a biometric match with that file. Analysis based on a single enrollment can be used to generate inclusion on a BEWL in certain cases (such as, latent prints connected with IEDs or other high-level crimes, positively identified high-value individuals, or positively identified associated individuals).

Uncertain (U)

7-15. (U) An *uncertain* response indicates that an automated determination cannot be made. Biometric match algorithms provide only a probability that two reference files match. Because the match threshold is adjustable, the comparison result may be too weak to respond with an automated match result. (The *match threshold* is the probability score at which a result is accepted as a match and below which a no-match/single encounter result is returned.) In ABIS, trained biometric examiners review uncertain match candidates and match or determine them as a no-match or single encounter.

Error (U)

7-16. (U) An *error* response is returned if there has been a processing error.

Note. (U) DOD DNA matches are processed outside of ABIS. In addition, facial and latent print matches are not automated and require a human examiner to make a determination.

BIOMETRIC COLLECTION CAPABILITIES (U)

7-17. (U) There are numerous biometric collection capabilities that enter biometric data into ABIS. To identify which no-match/single encounter and match reports are relevant, it is helpful for the analyst to have an understanding of the types of biometric collection devices or sensors. For example, BAT-A is a commonly used device employed in various settings, from employment screenings to enrollments of detainees.

Determining Significance of a Match (U)

(U) Often, a no-match/single-encounter response from BAT-A is insignificant. However, a match report from a BAT-A collecting data at a detention facility with a BAT-A enrollment for access may signify a potential protection threat.

(U) In this example, a particular combination indicates that a detained individual had also undergone an employment screening or request for base access. Several factors determine the significance of a biometric match, such as chronology and the identification date, or the date the match was made. In this example, the two BAT-A matches would be more significant if the BAT-A enrollment at the detention facility occurred prior to the BAT-A enrollment for access. This understanding is important for BEI analysis. Analysts must understand the operational context to know how to apply BEI to the specific mission.

BIOMETRIC STORAGE SOURCES (U)

7-18. (U) A *biometric storage source* is a database and infrastructure that stores biometric files. Storage requirements can be as complex as a data megacenter or as simple as a handheld device. When performing analysis, it is important to understand where the biometric data is coming from so the analyst can estimate its accuracy. There are three types of biometric storage sources:

- Authoritative.
- Local trusted.
- Local untrusted.

Authoritative Sources (U)

7-19. (U) An *authoritative source* is a Department-of-Defense-approved repository of biometric information. DOD may designate more than one authoritative source for various populations, as allowed by applicable law, policy, and directives. All DOD operational applications are designed to acquire biometric files from the appropriate authoritative source. ABIS is the primary DOD authoritative source. It provides a strategic capability for access to standardized, comprehensive, and current biometric files within DOD. It also allows for sharing biometric files with joint, interagency, and designated multinational partners.

Local Trusted Sources (U)

7-20. (U) A *local trusted source* is a subset of an authoritative source that is established at the operational level to accomplish a specific function in support of a mission. Reasons for establishing a local trusted source include insufficient network connectivity able to provide adequate access to the authoritative source or an operational need for closed-loop access or permission application.

Local Untrusted Sources (U)

7-21. (U) A *local untrusted source* is a local repository of biometric files that have not been enrolled with an authoritative or local trusted source. In many cases, local untrusted sources are established for missions of short duration or to satisfy political, policy, or legal restrictions related to sharing of biometric data. A host-nation fingerprint file is an example of a local untrusted source. Because of the potential unreliability of the information in local untrusted sources, they should be used sparingly and only when absolutely necessary.

BIOMETRIC SEARCHES (U)

7-22. (U) Although a biometric match might be the starting point for analysis, other intelligence reports may lead an analyst to search the appropriate databases to determine whether a person of interest has a

biometric file. Locating a biometric file enables the analyst to obtain further information on the individual and, if warranted, to nominate the individual for placement on the BEWL.

7-23. (U) Some biometric systems allow analysts the ability to search databases containing different types of biometric information (such as biometric characteristics, associated data, and contextual data) simultaneously. (b) (3)

(b) (3)

7-24. (U) BI2R also provides links to individuals associated with the person identified by a biometric file. This capability is helpful in confirming whether a particular biometric file belongs to the individual sought.

Determining an Identity Through Links (U)

(U) A HUMINT report lists an individual's associates by name. BI2R is searched and a biometric file believed to be that of the individual is linked to other individuals also mentioned in the report.

(U) Further analysis may confirm that the biometric file belongs to the subject of the HUMINT report. BI2R queries are conducted using identification numbers, names, and keywords. An enhanced search technique program can be used to further refine the query if the analyst knows more detailed data about the individual. Such data might be the specific location of a previous capture or the place of birth.

(b) (3)

LINKING BIOMETRIC FILES WITH REPORTING (U)

7-25. (U) All related reporting is attached to the biometric file in BI2R to provide a history of encounters and interactions with that person. For example, if an individual is captured as a result of intelligence reporting linking the individual to insurgent activity, the following tasks occur: the individual's biometric samples are collected, a biometric file is created or updated, and the intelligence reporting that led to the targeting of the individual is linked to that biometric file. If the actual reporting document cannot be attached to the biometric file, the associated reporting should be referenced within that file. Associated documents greatly assist the analyst in conducting a more thorough and accurate BEI assessment.

7-26. (U) Collectors may also input additional data during biometric enrollments. Examples of additional data include—

- Scanned images of any identification cards.
- Pocket litter.
- Names and identification numbers of any other individuals detained at the same time and location.
- A significant activity report detailing the events of the capture.
- Photographs taken during the capture.

7-27. (U) Following the BEI process allows analysts to link intelligence with biometrically derived contextual data and a biometric sample to generate an all-source product. (See figure 2-2 on page 2-4.) To complete analysis, analysts may perform further research to locate other related reporting on the individual or network of interest. Information is available across NIPRNET, SIPRNET, and JWICS. Common databases and Web sites used to conduct biometric research are listed in appendix A.

7-28. (U) One technique for linking biometric information with reporting is creating persistent files. A persistent file correlates the biometric and associated data with other available information on an individual. The file allows derogatory reporting to follow the individual throughout the detention cycle, helping to prevent inadvertent or a premature releases of high-threat individuals.

ANALYZING DETAINEE INFORMATION (U)

7-29. (U) Detention operations are a function of the military police community. Detainees frequently possess valuable, even indispensable, information that intelligence analysts need for developing the current situation and for answering priority intelligence requirements. Because of this, biometric enrollments of detainees should always be evaluated. With an account and the appropriate privileges, analysts can access a detainee tracking system, which may maintain files of tens of thousands of detainees in holding areas and joint force detention facilities. Moreover, analysts should develop positive working relationships with personnel working at detention facilities, such as military police and HUMINT collectors. These relationships are especially useful during counterinsurgency and stability operations.

7-30. (U) A detainee tracking and management system capability is a Web-accessible automated information system that provides data to analysts seeking information of intelligence value. An internment serial number is generated whenever an individual is interned in a detention facility, providing a common reference number in associated biometric collection devices and detainee management systems. The information in this management system is used to track detainees within and between detainment facilities, as well as record their daily events and other information, such as medical problems, visitor requests, and behavioral problems. (See FM 3-63 for more information about detainee operations.)

7-31. (U) Information such as familial associations, biographical data, and associated capture tags are recorded when a detainee is biometrically enrolled with a BAT-A. This data is then stored in the detainee's biometric file, which can be accessed by the detainee tracking and management capability. Detainee information that is useful to an analyst evaluating biometric data includes—

- Capture tags.
- Screening information.

- Property analysis.
- Interrogation plans and summaries.
- Intelligence information reports.
- Legal adjudication information.

ANALYTIC SUPPORT TOOLS AND TASKS (U)

7-32. (U) Analytic support tools reduce the time needed to analyze and identify an individual who is a threat or may have intelligence value. These systems and tools are used to provide feedback to the collector, analyst, and consumer about the identity of the individual and on whether further action is necessary. The intelligence staff uses these tools to support recommendations to the commander and operations staff. The information gained about an individual can lead to other insights too, such as threat units in the area, battle damage assessment, threat tactics and techniques, and threat objectives or goals. Obtaining the information needed to produce intelligence through analysis depends on continuous and methodical planning and evaluation throughout the intelligence process. Ultimately, the analyst decides which tools are most effective for the operational environment. Some of the tools used and tasks performed include—

- Biometric named area of interest products.
- Targeting.
- Event templates and event matrices.
- Link diagrams.
- Density plot map overlays.
- Battle damage assessment charts.
- Database analysis.

BIOMETRIC NAMED AREAS OF INTEREST PRODUCTS (U)

7-33. (U) A *named area of interest* is the geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of adversary courses of action (JP 2-01.3). Named areas of interest may also be related to conditions of the operational environment. Analysis of significant events and the geospatially tagged data helps determine areas where biometric collection efforts would be most useful. These areas are designated as named areas of interest. They are combined with other intelligence information to create biometric named area of interest products.

7-34. (U) A biometric named area of interest product is designed for the purpose of driving targeted biometric enrollments. This product consists of a recommended area of interest, a list of persons of interest believed to be in that area, and supporting analytical products. Analysts incorporate all-source capabilities—such as HUMINT, significant activities, forensically exploited evidence, and the location of biometric enrollments—to develop a product that provides recommendations as to where units are most likely to encounter persons of interest. While primarily used to recommend areas where biometric enrollments should be conducted, the biometric named area of interest product is also used to identify areas where the collection of evidence is a priority in order to identify individuals involved in threat activity. The final product provides analysis on the recommended named areas of interest, highlights individuals who have either been enrolled or have been biometrically matched to evidence within that area, and contains various density maps that outline the data used to conduct the analysis.

TARGETING (U)

7-35. (U) Intelligence Support to Targeting and Information Superiority is the task of providing the commander information and intelligence support for targeting lethal and nonlethal actions. (See FM 7-15.) Biometric information and BEI are critical contributors to targeting. They provide initial targets and persons of interest based on researched databases and detailed IPB. During combat operations, biometrics

can verify the identity of individuals who would otherwise be considered noncombatant civilians, which can ultimately lead to the targeting of additional threat individuals.

EVENT TEMPLATES AND EVENT MATRICES (U)

7-36. (U) Event templates and matrices support biometric collection and BEI by displaying how a certain threat entity normally behaves during a specific set of circumstances in time and space. Event templates and matrices ensure a consistent and well-reasoned portrayal of threat capabilities throughout planning. They are critical in tying information collection and the supported unit's concept of operations together. By understanding and utilizing event templates and matrices, analysts can provide better information for the intelligence staff to use in biometric collection planning. Better planning contributes to more effective collection which, in turn, leads to more timely and relevant analysis.

LINK DIAGRAMS (U)

7-37. (U) Link diagrams enable the process of identifying and analyzing relationships among personnel, contacts, associations, events, activities, organizations, and networks to determine significant links. Analysts use link analysis to determine who is involved, how they are involved, and their significance concerning a particular situation. Some types of link analysis tools include—

- Association matrices.
- Activity matrices.
- Link diagrams.
- Network diagrams.

7-38. (U) When performing link analysis, a biometric match result supports targeting and interrogations. A biometric match can be instrumental in enabling and supporting an all-source analytical conclusion regarding associations and linkages. (See ATP 2-33.4 for link analysis techniques.)

DENSITY PLOT MAP OVERLAYS (U)

7-39. (U) A density plot map is a geospatial tool (overlay or template) that depicts areas of concern for a given activity, such as IED events, biometric enrollments, and watch list encounters. Density plots are symbols depicting events, situations, personnel, organizations, and installations with the supporting data needed to enable users to display and understand the symbols. The tool is used as an all-source analysis aid and is not specific to biometrics.

BATTLE DAMAGE ASSESSMENT (U)

7-40. (U) *Battle damage assessment* is the estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force (JP 3-0). Battle damage assessment is one of the most important and difficult tasks an analyst performs. It is important because accurately determined battle damage assessment can reveal current enemy strengths and vulnerabilities. It is difficult because determining the amount of equipment destroyed, the number of enemy captured, or the level of degradation inflicted on an enemy unit can be very challenging. Biometrics and BEI can contribute to this task by, for example, verifying the identity of an enemy prisoner of war with direct knowledge of the attack being assessed. BEI can also verify the identities of deceased personnel in a target area, confirming the death of threat leaders and other high-value individuals.

DATABASE ANALYSIS (U)

7-41. (U) Databases such as BI2R are vital to BEI analysis. Real-time collaboration, detailed operational planning, and planning requirements and assessing collection, as well as enhanced collection and source exploitation tools, all support analysis. Emerging technology is increasing the value and relevance of the BEI analysis system.

ASSESSING BEI ACTIVITIES (U)

7-42. (U) Assessment is an activity of the operations process. For intelligence purposes, assessment involves the continuous monitoring and evaluation of the current situation, particularly significant threat activities and changes in the operational environment. Assessing the situation begins upon receipt of mission and continues throughout the operation and during all steps of the intelligence process. (See ADRP 2-0.) One source of information used for assessment is feedback.

7-43. (U) Feedback provides intelligence planners, collectors, analysts, and disseminators with the opportunity to improve the BEI process, refine collection and production requirements and priorities, and capture best practices and lessons learned. Throughout the BEI process, there is continuous assessment based on evaluation and feedback.

7-44. (U) Criteria expressed in the forms of measures of effectiveness and measures of performance aid in making assessments. Measures of effectiveness help determine if a task is achieving its intended results. Measures of performance help determine if a task is completed properly. (See ADRP 5-0.) Factors to consider when establishing measures of effectiveness and measures of performance for biometrics and BEI include the following. While this list is not all inclusive, it provides a framework of things to consider when assessing how biometrics are being used to support commanders:

- Are biometric information and BEI effectively integrated into the planning and directing step of the intelligence process?
- Are biometric information and BEI effectively integrated into the information collection plan?
- Do biometric information and BEI contribute to answering commanders' intelligence requirements?
- Do biometric resources (such as, BAT-A, tactical handheld biometric collection devices, and the biometric architecture) meet unit needs?
- Are Soldiers collecting biometrics as specified in DOD standards?
- Do biometric collection efforts negatively impact local perceptions of friendly operations? (No is good.)
- Are biometric data and BEI disseminated in a timely manner and to the appropriate personnel and units?
- Do positive relationships exist with other biometric personnel, organizations, and agencies?
- Is full advantage taken of other agencies' biometric capabilities?
- Are biometric lessons learned disseminated?
- Are changes made based on disseminated lessons learned?

7-45. (U) Once biometric data has been disseminated, analysts maintain visibility on specific persons of interest as part of continuous assessment. Additionally, metrics in the form of measures of performance and measures of effectiveness are available through biometric systems and databases to assess the entire range of BEI activities. These can answer questions like—

- How well do the analysts and collectors perform?
- Are the analysts and collectors doing the right things to achieve the desired outcome?

PART THREE

Biometric Considerations for Different Missions and Operations (U)

Chapter 8

BEI Support to Decisive Action (U)

(U) Army forces conduct decisive and sustained land operations through the simultaneous combination of offensive, defensive, and stability operations (or defense support of civil authorities within the United States and its territories). This chapter discusses how biometric information and BEI support intelligence development during each of these actions.

OFFENSE (U)

8-1. (U) Biometric information and BEI give commanders a better understanding of specific individuals, civil and military leaders, organizations, and threats to friendly forces. As offensive tasks are executed, newly collected biometric information and BEI from enemy prisoners of war, deceased combatants, site exploitation, and other sources enhance commanders' situational understanding in a fluid environment. Biometric information and BEI may not be easily collected during offensive tasks; however, they are valuable intelligence multipliers that should be sought as circumstances and resources allow.

8-2. (U) Generate Intelligence Knowledge is a continuous, user-defined task driven by the commander. (See FM 7-15.) It begins before mission receipt and provides the relevant knowledge required for the conduct of operations. The information collected and intelligence produced are refined into knowledge for use in IPB and other mission analysis tasks.

8-3. (U) It is critical to include biometric information and BEI planning during initial IPB to support answering the commander's intelligence requirements during offensive operations. Biometric information and BEI, when integrated into all-source analysis, helps the intelligence staff do the following:

- Add clarity to understanding the threat through database research during IPB.
- Confirm or deny specific units by identifying select individuals.
- Confirm or deny threat courses of actions by identifying individuals who are part of specific units.
- Identify military, community, and other leaders in the area of operations.
- Support targeting of high-value individuals.
- Confirm identities through deceased individual forensic analysis.
- Enhance situational development when transitioning to the defense or stability operations.

8-4. (U) Biometric analysis support from other agencies may be difficult for analysts to obtain due to organic intelligence and communications architecture limitations. Intelligence staffs should preload biometric information and BEI historical data. They need to be able to perform analysis and develop intelligence when communications are degraded or lost. A current biometric database, BEWL, and updated biometric collection devices can help achieve this objective.

DEFENSE (U)

8-5. (U) Analysts plan how biometrics and BEI support answering commanders' intelligence requirements during initial IPB and operations and intelligence planning. Biometric collection is easier to execute and BEI easier to develop during the defense. This is because units are maneuvering less, thus allowing for better collection and exploitation of biometric information. A stable environment also allows for better connectivity and more reliable dissemination procedures. BEI supports defensive tasks through—

- Recommending surveillance and lethal and nonlethal targeting of high-value individuals.
- Confirming and denying specific units by identifying select individuals.
- Confirming and denying threat courses of actions by identifying individuals who are part of specific units.
- Identifying military, community, and other leaders in the area of operations.
- Building a local biometric database, as operations permit.
- Confirming battle damage assessment and identities through deceased individual forensic analysis.
- Enhancing situational development when transitioning to the offense or stability operations.

8-6. (U) During peace operations, irregular warfare, and military engagement, the conduct of a unit defense is closely related to perimeter defense and base security. The integration of biometric collection and BEI analysis enables success during defensive tasks and a smooth transition to stability operations.

STABILITY (U)

8-7. (U) Army forces have been conducting stability tasks in multiple countries for many decades. As a result, the use of biometric information and the development and use of BEI have evolved considerably. Biometric information is collected during various tasks common in a stability environment, such as base security operations, village support operations, and traffic control operations. BEI is valuable to commanders in a stability environment because it can lend detailed insight into threat individuals, threat groups and organizations, population attitudes toward friendly forces, and threat characteristics and patterns. When BEI is fused into all-source intelligence during stability operations, it supports the commander's situational understanding by contributing to a multidisciplined intelligence picture.

8-8. (U) During stability missions, commanders often require detailed intelligence and IPB products to determine how best to conduct operations and influence the local population. A lack of knowledge concerning insurgents, local politics, customs, culture, and how to differentiate between the local population and combatants often leads to actions that can result in unintended and adverse consequences. Consequences can include attacking unsuitable targets or offending or causing mistrust among the local population. Integrating biometric information as part of all-source analysis during intelligence and operational planning can help set the stage for success in a stability environment.

DEFENSE SUPPORT OF CIVIL AUTHORITIES (U)

8-9. (U) *Defense support of civil authorities* is support provided by U.S. federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law

enforcement support, and other domestic activities, or from qualifying entities for special events (DODD 3025.18).

8-10. (U) Four core tasks are associated with defense support of civil authorities:

- Provide support for domestic disasters.
- Provide support for domestic civilian law enforcement agencies.
- Provide support for domestic chemical, biological, radiological, or nuclear incidents.
- Provide other designated support (national special security events, critical infrastructure protection, or other events).

8-11. (U) Biometric information is most helpful in supporting civilian law enforcement agencies. (See ADRP 3-28 and ATP 2-91.7 for information on defense support of civil authorities.)

Note. (U) All Army intelligence support to civil authorities must be authorized and comply with all laws and regulations, including EO 12333 and AR 381-10.

This page intentionally left blank.

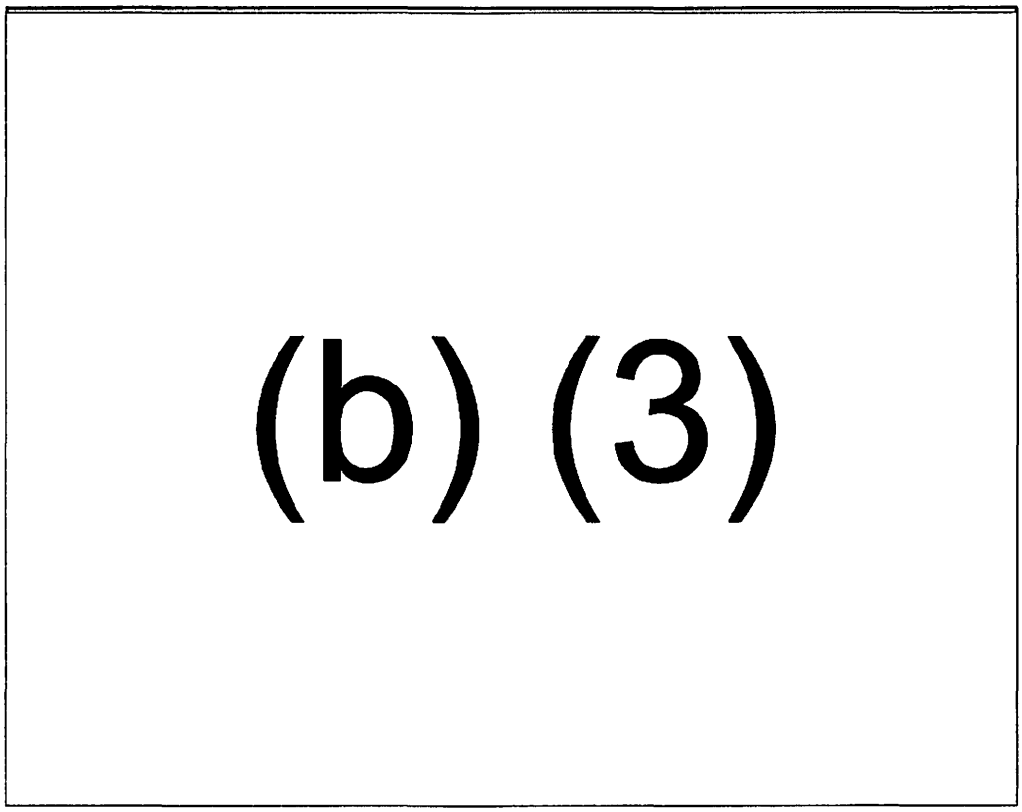
Chapter 9

BEI Considerations for Specific Operations, Missions, and Environments (U)

(U) Although many biometric tasks and BEI processes remain constant across the range of military operations, there are special considerations and techniques that are advantageous during specific operations and environments. This chapter contains several vignettes illustrating how biometrics can be a critical enabler of many diverse missions throughout the range of military operations. Analysts need to be aware of the techniques involved in effectively integrating biometrics into the intelligence process, thereby ensuring BEI is included in the overall intelligence picture. Ultimately, commanders are responsible for ensuring biometrics is integrated into intelligence and operational planning and for ensuring biometric capabilities are fully used. Another aspect of this responsibility is ensuring the unit understands and is trained on biometric collection devices.

BORDER OPERATIONS (U)

9-1. (U) Biometric information is effective in tracking cross-border movements. Biometric information can contribute to limiting the corridors a threat may use to access operational areas.



(b) (3)

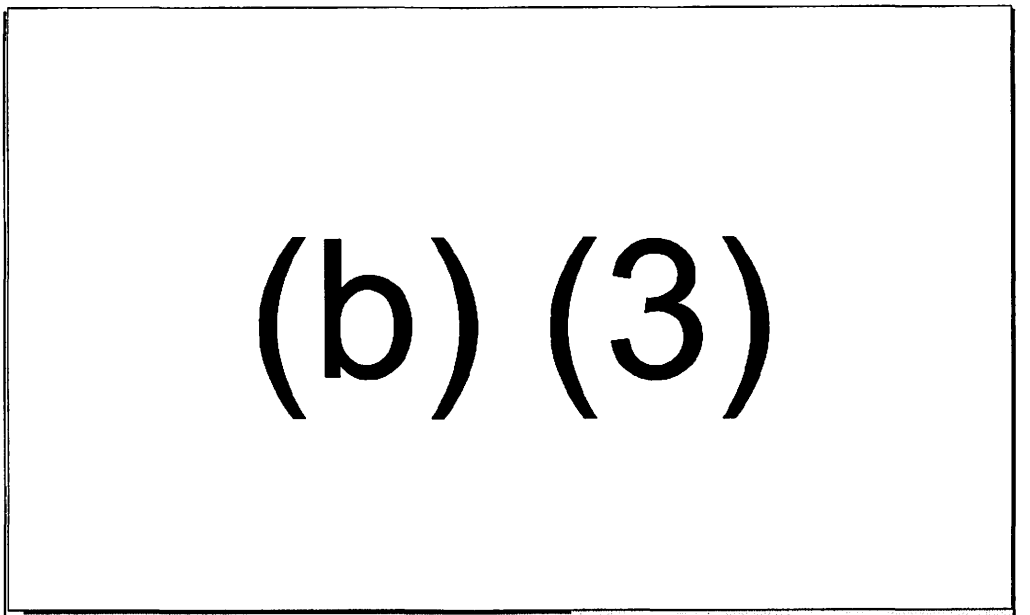
(U) This vignette illustrates the following tasks performed using biometrics:

- Identify an individual during tactical operations.
- Locate a person of interest.
- Track a person of interest.
- Control physical access.
- Share biometric information.

CONTRACTING IN A FOREIGN NATION (U)

9-2. (U) Contracting in a foreign nation can be complicated; however it is necessary to the success of U.S. operations. Often there are critical operational support tasks that Army forces may not be able to accomplish effectively themselves. In these cases, commanders attempt to hire local businesses to perform these tasks. Another positive outcome of hiring local businesses is supporting the local economy. However, there are considerations commanders need to be aware of, including how biometrics can support contracting operations.

(b) (3)



(U) This vignette illustrates the following tasks performed using biometrics:

- Track a person of interest.
- Control physical access.
- Enable information assurance (authorize access to privileges).
- Share biometric information.

CORDON AND SEARCH (U)

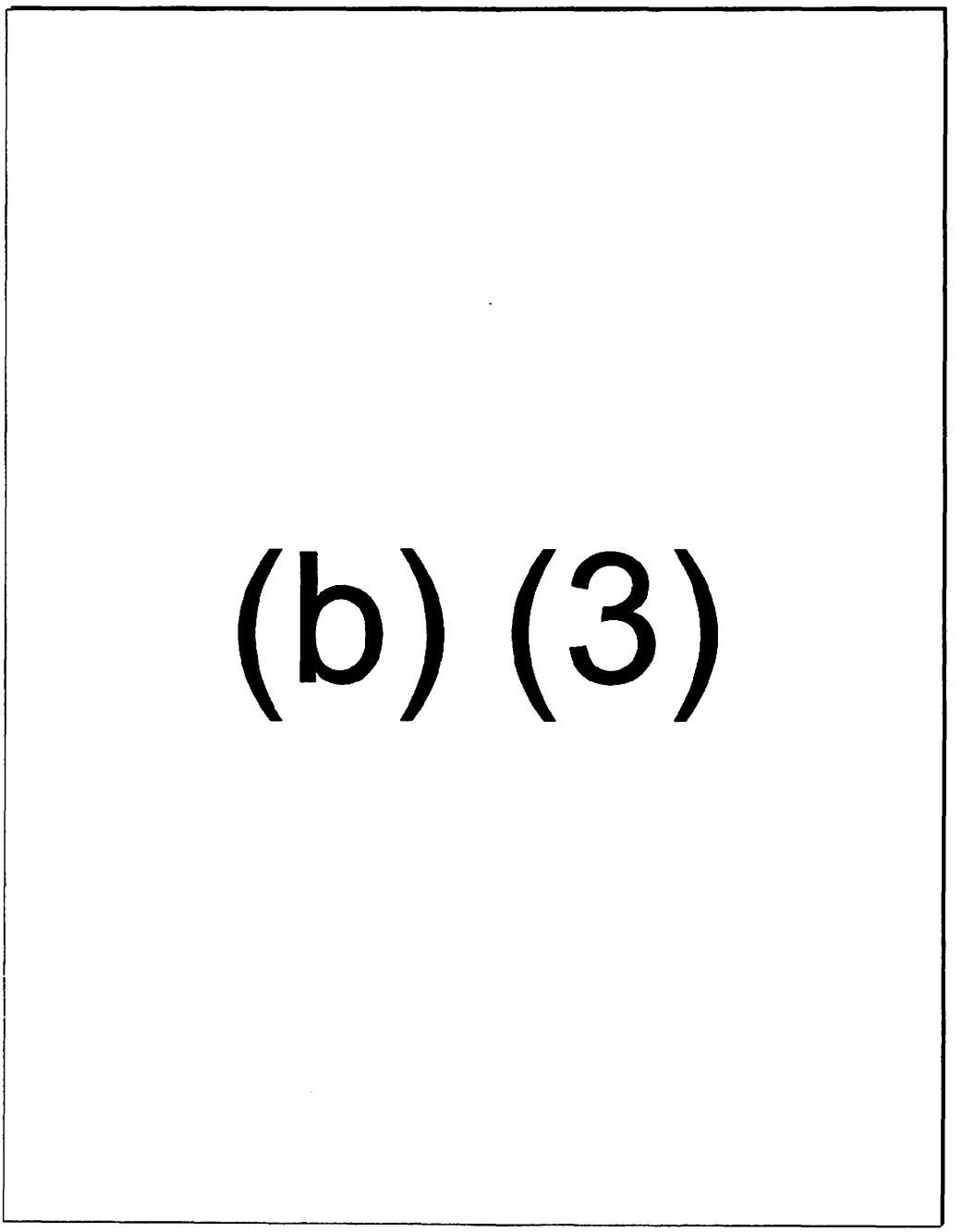
9-3. (U) *Cordon and search* is a technique of conducting a movement to contact that involves isolating a target area and searching suspected locations within that target area to capture or destroy possible enemy forces and contraband (FM 3-90-1). Cordon and search operations take place throughout the range of military operations.

9-4. (U) There are two primary elements in a cordon and search operation—the cordon element and the search element. Both elements have requirements for biometric and forensic capabilities. The search team may use several approaches to the search itself, including central assembly and restriction to quarters, or control of the heads of households. In each of these approaches, biometric information can be used effectively. The cordon element can set up checkpoints in which traffic control detachments with biometric collection capability are used to screen individuals seeking to enter or leave the cordon area.

9-5. (U) Planning considerations are—

- Include biometric capability instructions in operation and fragmentary orders.
- Plan to perform biometric enrollments and screening of everyone, if possible.
- Ensure current watch lists and local alerts are loaded before mission execution.
- Ensure biometric support Soldiers with traffic control detachments have extra charged batteries for completion of the mission.
- Ensure Soldiers are trained in site exploitation activities and have the appropriate equipment.
- Document and associate all items found during site exploitation activities with individuals at the site.
- Plan for positive or negative identification of personnel.
- Coordinate transportation for detained personnel and items found at the site.

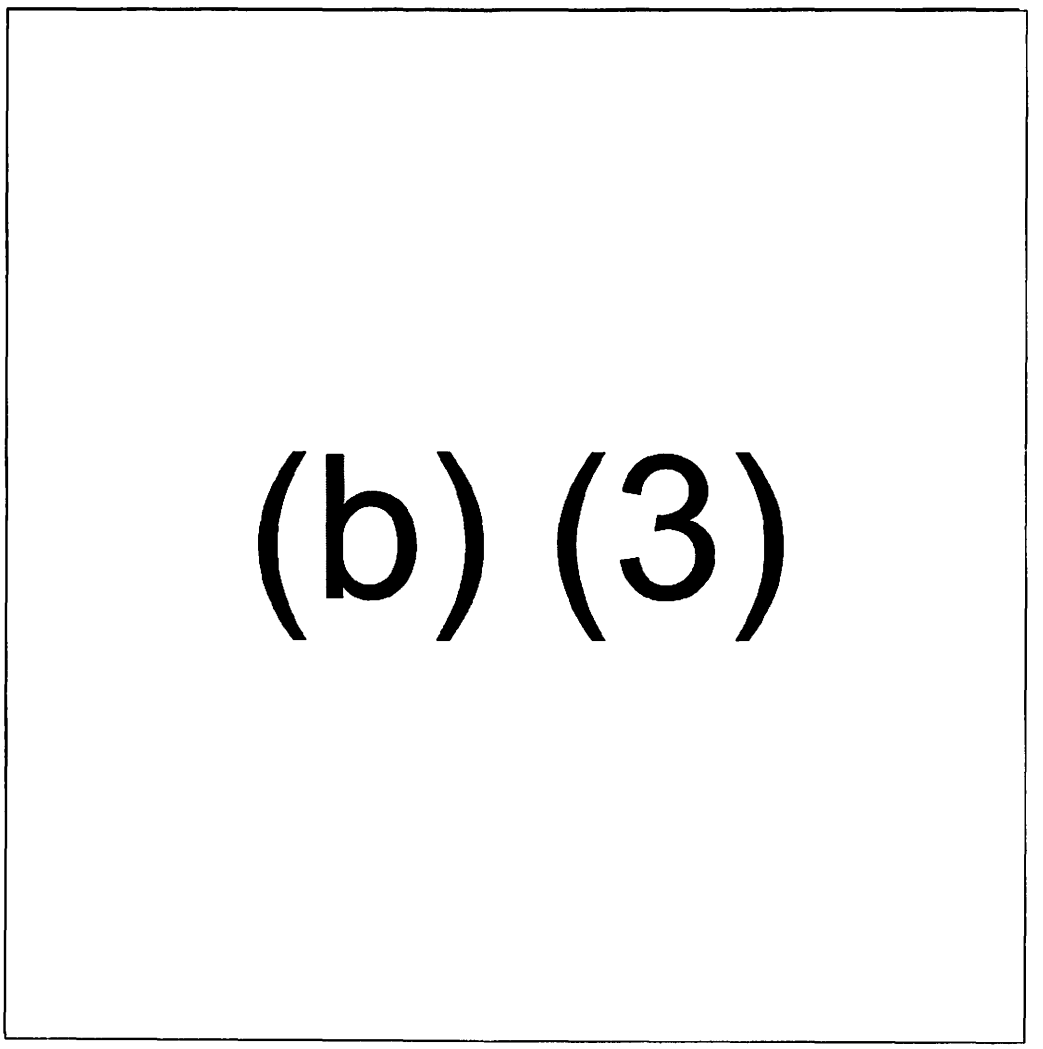
- Ensure Soldiers are trained to use the tactical handheld biometric collection device.
- Use traffic control detachments with biometric collection capability at checkpoints in the cordon to canalize traffic.
- Incorporate biometric information into debriefs.
- Enroll everyone, to include all wounded in action and killed in action.
- Conduct internal after action reviews of biometric actions.

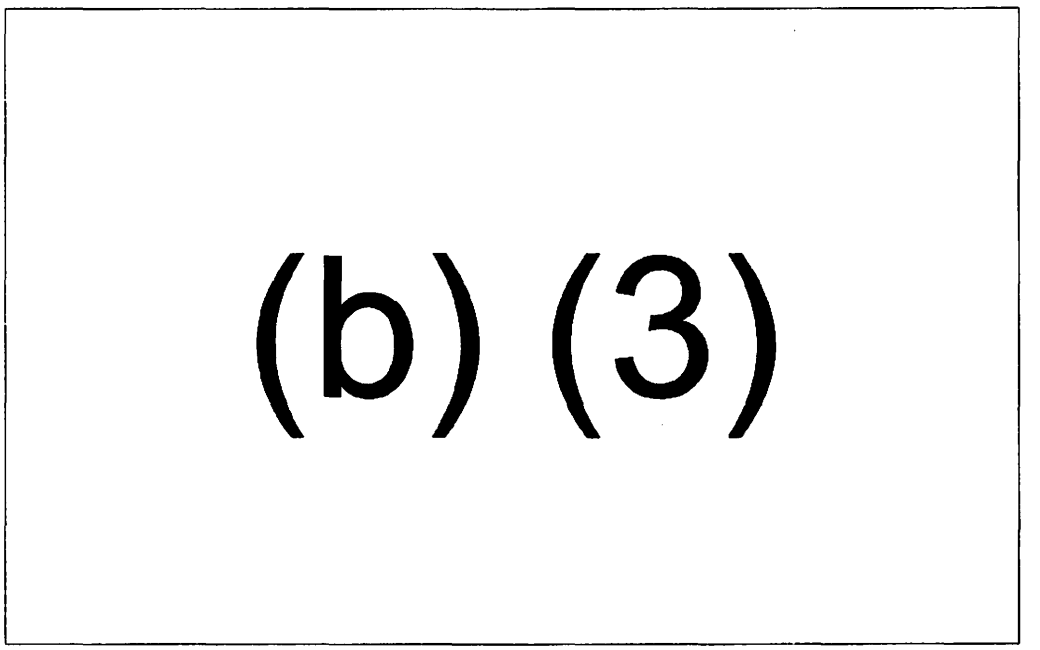


AREA DEFENSE (U)

9-6. (U) Defensive operations can present many challenges and positive opportunities for commanders. The fact that a unit is conducting defensive operations could mean the commander is facing a lull in the battle and offensive operations will begin again soon, or it could suggest that the unit will transition into stability operations. In both instances, intelligence analysts need to be prepared to integrate biometric information and BEI into intelligence and operational planning.

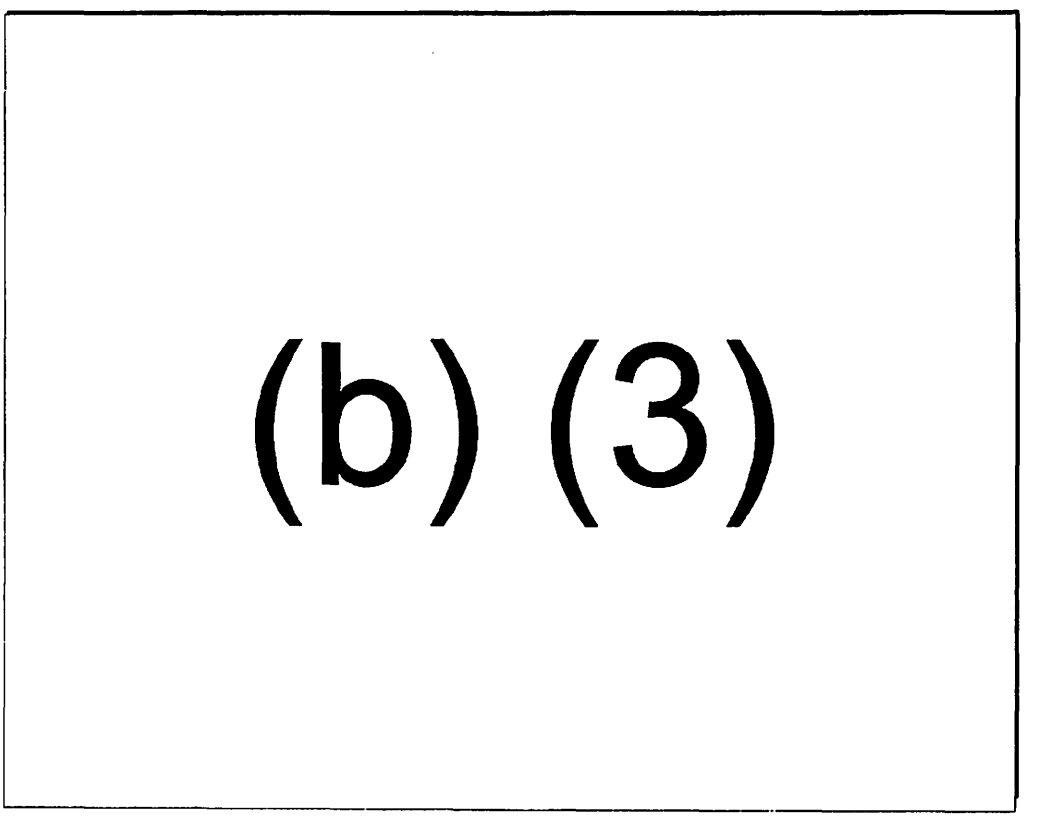
9-7. (U) The *area defense* is a defensive task that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright (ADRP 3-90). The following vignette provides an example of how biometrics and BEI can support an area defense.





DISASTER RELIEF (U)

9-8. (U) Initial support operations in response to disasters can be challenging. Biometric information can be very useful in helping to identify victims and other personnel encountered during these operations.



(b) (3)

(U) This vignette illustrates how biometrics can contribute to managing emergency situations.

LOCALLY EMPLOYED PERSONNEL SCREENING (U)

9-9. (b) (3)

(b) (3)

9-10. (b) (3)

(b) (3)

9-11. (b) (3)

(b) (3)

9-12. (b) (3)

(b) (3)

9-13. (b) (3)

(b) (3)

9-14. (b) (3)

(b) (3)

9-15. (b) (3)

(b) (3)

9-16. (b) (3)

(b) (3)

MARITIME INTERDICTION (U)

9-17. (U) As recent operations have shown, Army forces must be prepared to conduct operations with other Services and government agencies. It is critical for all of these elements to share biometric information quickly and accurately. Biometric information collected in remote Army operational areas can become critical information and intelligence that supports maritime operations around the world.

(b) (3)

(U) This vignette illustrates the following tasks performed using biometrics:

- Identify an unknown individual during tactical operations.
- Locate a person of interest.
- Track a person of interest.

PERSONNEL RECOVERY (U)

9-18. (U) The importance of collecting and sharing biometric data throughout the Services and government agencies becomes clear when data is used to support personnel recovery operations. *Army personnel recovery* is the military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel (FM 3-50). Recovery operations may be planned or occur in conjunction with other operations. A unit may be actively seeking a U.S. service person held as a prisoner or a hostage in an area, or may simply find them in the course of an operation. (See FM 3-50 for personnel recovery doctrine.)

Personnel Recovery Vignette (U)

(U) U.S. Government, DOD, multinational, and nongovernmental organizations personnel are conducting stability operations in a country coping with insurgent activity. Several civilians have been abducted.

(U) A U.S. special operations force team receives information from intelligence sources concerning the location of a U.S. civilian contractor who has been held by insurgents for nearly 30 days.

(U) Since the captive is a U.S. person, the operational commander requests the biometric file on the captive. The data is provided and downloaded to the unit's tactical handheld biometric collection devices.

(b) (3)

(U) The team initiates handling protocols for the rescued captive and detains the remaining individuals. At the repository, the files are processed and stored for future use.

(U) Tasks achieved using biometrics during this operation are—

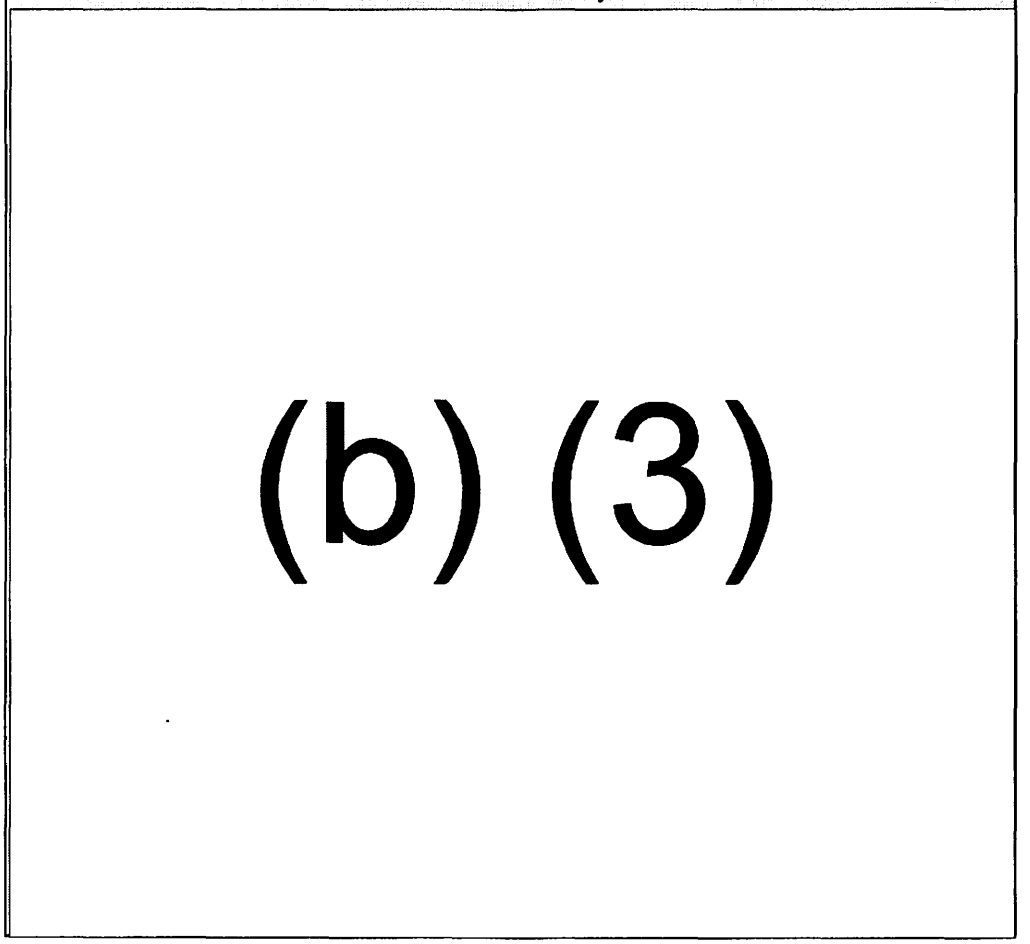
- Identify an individual during tactical operations.
- Locate a person of interest.
- Identify friendly forces.

PROTECTION (U)

9-19. (U) *Protection* is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (JP 3-0). Biometrics enables protection missions by providing U.S. forces with a screening tool for individuals with access to U.S. facilities. Biometric matches can be used to help in the vetting process. An effective vetting process can help determine an individual's potential threat level, which can then be used to help the commander decide an individual's access to U.S. and multinational forces' facilities.

Protection Vignette (U)

(U) Alpha Company has achieved all of its operational objectives and is ordered to start conducting stability operations in the eastern and southern sectors of a large city. Charlie Company is securing its own position and conducting similar operations in the western and northern sectors of the same city.



TARGETING (U)

9-20. (U) *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting helps the staff and targeting working group decide which targets must be acquired and engaged. The Army targeting methodology comprises the functions decide, detect, deliver, and assess (also called D3A). (See ATP 3-60.)

9-21. (U) Targeting is an outgrowth of the commander's decisions and establishes the requirements for developing effective information collection and intelligence operations efforts. Intelligence operations support the targeting process by—

- Locating targets.
- Identifying, classifying, and tracking targets.
- Observing actions on targets.
- Determining whether to engage or continue collection on targets.
- Assessing the effects of those actions.

9-22. (U) Military intelligence collection assets collect information to aid in performing the following tasks: situation development, target acquisition, functional damage assessment, munitions effects assessment, and battle damage assessment. However, many collection assets cannot support all these tasks at the same time. Therefore, prioritizing the information collection tasks given to them is critical. (See FM 2-0 and ATP 2-01.)

9-23. (U) The find, fix, finish, exploit, analyze, and disseminate (F3EAD) methodology is the primary means for engaging high-value individuals. The targeting aspect of F3EAD is consistent with the decide, detect, deliver, and assess methodology; moreover, F3EAD provides maneuver commanders an additional tool to address certain targeting challenges, particularly those found in a counterinsurgency environment. (See figure 9-1.) F3EAD is not a replacement for decide, detect, deliver, and assess; nor is it exclusive to targeting. It is a specific technique that works best at the tactical level for helping leaders understand their operational environment and visualize the effects they want to achieve.

9-24. (U) Thorough planning and disciplined execution helps commanders employ high-demand military intelligence collection assets more efficiently. Biometric information enables targeting by helping to positively identify individuals. For example, a biometric enrollment sent to ABIS may help identify the individual who is on the BEWL. An alert text can inform the collector of such a match.

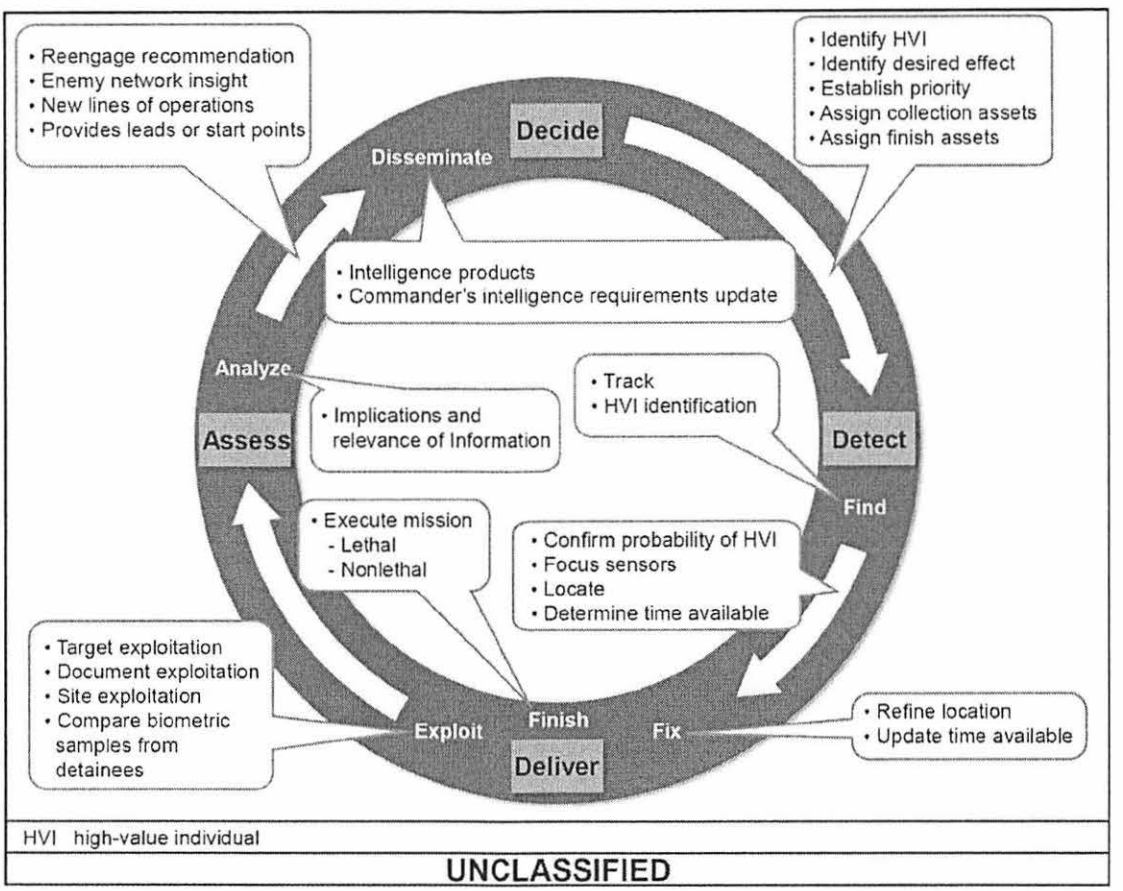
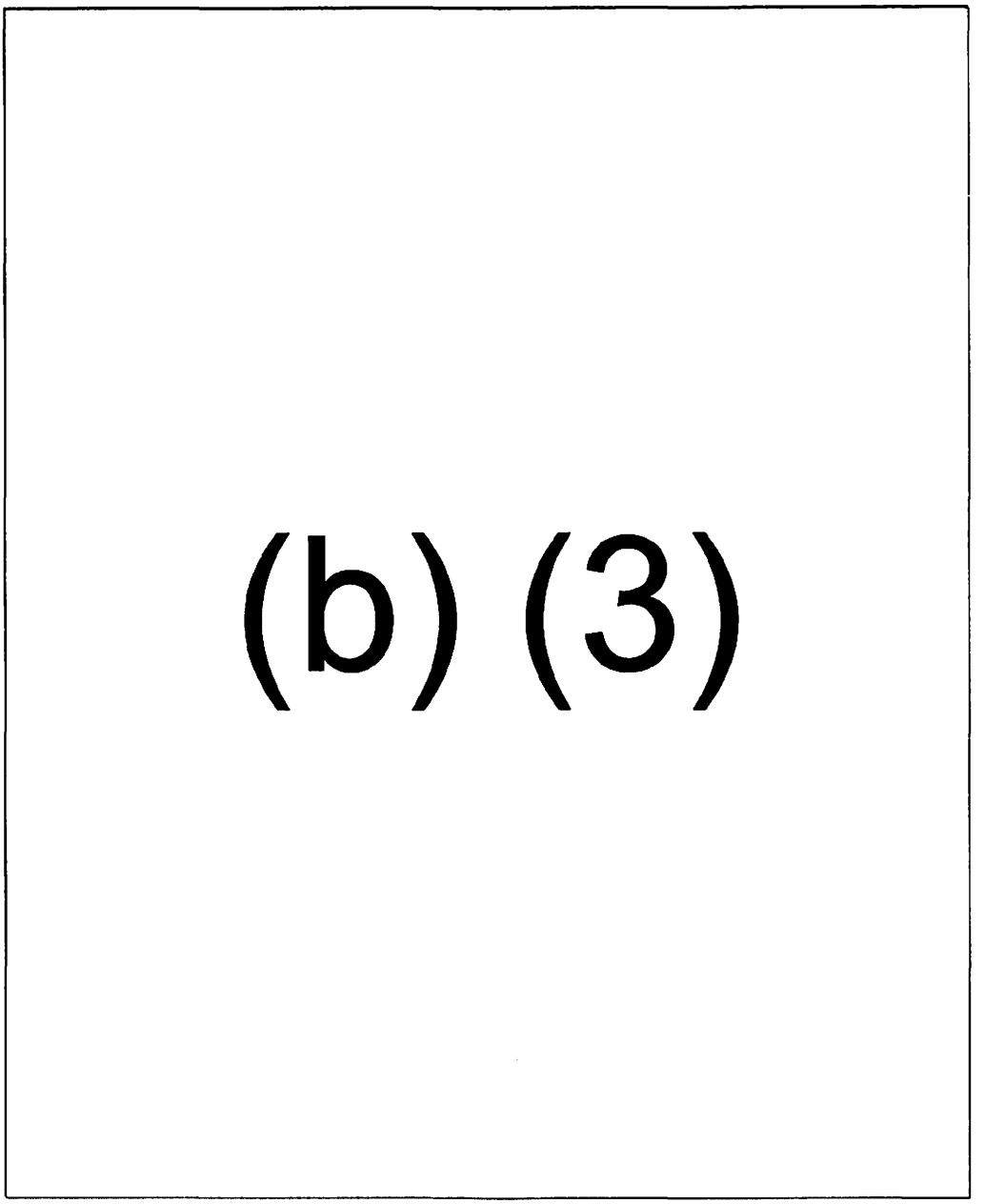


Figure 9-1. (U) BEI contributions to the high-value individual targeting process



THEATER SECURITY COOPERATION AND EXERCISES (U)

9-25. (U) The U.S. military can further security cooperation through civic action programs in remote regions of partner nations in conjunction with port visits and multinational military exercises. The following vignette describes one way biometric capabilities can contribute to the success of these programs.

Theater Security Cooperation and Exercises Vignette (U)

(U) During an annual multinational exercise, an Army medical detachment executes medical civic action programs in a number of villages within the exercise area. Army medics collect biometric data on those who receive vaccinations and medical treatment during the medical civic action programs. The biometric data is collected with consent from the patients and the host-nation government. Biometric files are enrolled and stored for each individual receiving treatment or vaccinations. These biometric files are linked to subsequent treatment and vaccination records stored in other repositories of associated information.

(U) The following year a different Army medical detachment deploys to the same area to perform a medical civic action program. At the first village, Army medics encounter far more villagers awaiting vaccination than anticipated, creating concern that the amount of on-hand vaccine is insufficient. Biometric samples are collected on each person awaiting vaccination and matched to the local-trusted source. Numerous positive matches occur. These match results are compared against the repository of associated data to identify which individuals received vaccinations in the past. Analysis of the match results and the repository of associated data reveals that a large number of those awaiting vaccination have already received the vaccine during previous medical civic action programs and do not require an additional dose.

(U) Relying on the biometric data, the on-scene commander orders vaccination of only those with no biometric match and those with biometric matches whose linked medical treatment record does not indicate the vaccine was previously received. The villagers are briefed accordingly.

(U) The Army medics successfully complete the medical civic action program with the vaccine on hand. The on-scene commander is confident that the total supply of vaccine is sufficient for future medical civic action programs based on the biometric matches experienced in this initial medical civic action program. This vignette illustrates the task: Share biometric information.

WAR CRIMES PROSECUTION (U)

9-26. (U) War crimes can be extremely difficult to prosecute, but biometric data can be an invaluable asset during preparation and execution of this task. Biometric information can enable identifying deceased personnel, possibly establishing that war crimes were committed. Biometric information can also be used to identify war crimes suspects hiding among the populace.

War Crimes Prosecution Vignette (U)

(U) The United States and multinational partners have begun combat operations after several months of intense diplomatic activity. They are acting under a United Nations resolution authorizing the use of force. Their purpose is to defeat a country's invasion of one of its neighbors.

(U) The multinational force takes a large number of prisoners of war early in the campaign. Facial photographs and fingerprints are taken from the prisoners in order to provide friendly forces and appropriate international organizations an accounting of the identity of the prisoners, their health, and their location. The fingerprints and photographs are also enrolled into DOD's biometric database.

(U) Several mass graves are discovered by the multinational force, as liberation of the country continues. Latent fingerprints are recovered from spent shell casings using forensic techniques and matched to twenty enemy prisoners of war. When questioned concerning the presence of their fingerprints on the shell casings at the

mass graves, roughly half of the prisoners decline to answer or are highly evasive. The other half admit to their participation in the mass killings but state they were acting under coercion. Their accounts of the times and locations of the atrocities confirm evidence obtained through exploitation of captured documents. The cooperating prisoners identify several commanders as responsible for the atrocities and identify them from media footage. These commanders are also identified by multiple members of the local civilian populace as being responsible for the mass killings and theft.

(U) Preconflict photographs of the individuals suspected of ordering and leading the atrocities are electronically compared to the facial photographs of enemy prisoners of war under the multinational force's control. This results in two matches. When confronted, both individuals admit they presented false identity documents upon capture claiming to be members of the medical service corps. They state they did this in order to protect their knowledge of their country's military and intelligence apparatus. When questioned regarding illegal killings and looting, both individuals quickly claim no knowledge of such things and decline to answer further questions.

(U) After further evaluation and considering its conclusions, the United Nations Security Council refers the case to the International Criminal Court. By the end of hostilities, the International Criminal Court has issued several indictments for the individuals, who are later successfully prosecuted.

(U) Tasks achieved using biometrics are—

- Locate a person of interest.
- Share biometric information.

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(3) 50 USC §3024(i)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 83-85

IAGPA-CSF Form 6-R
1 Sep 93

This page intentionally left blank.

Appendix B
Biometric Modalities (U)

(U) There are varying levels of reliability and accuracy of biometric modalities based on the technology of the systems used to collect and exploit them. This appendix describes factors to consider during biometric collection and factors that affect the reliability and accuracy of biometric samples.

CONSIDERATIONS FOR COLLECTING DIFFERENT MODALITIES (U)

B-1. (U) Fingerprints, DNA, iris images, and facial images are the most widely used biometric modalities throughout DOD. Additionally, voice recognition is used. Although the mission and availability of collection systems dictate which modalities are collected, a basic understanding of the functionality and limitations of each modality is useful.

FINGERPRINTS (U)

B-2. (U) For more than a century, fingerprints have been one of the most highly used methods for human recognition. Automated biometric systems have only become available in recent years. The determination and commitment of the fingerprint industry, government evaluations and needs, and organized standards bodies have led to the next generation of fingerprint recognition technology. This promises faster and higher quality acquisition devices to produce higher accuracy and more reliability. Fingerprints have a generally broad acceptance with the general public, law enforcement, and the forensic science community.

B-3. (U) A friction ridge is a raised layer of skin found on a person's hands or feet. A fingerprint is a detail of the friction ridges of an individual's finger. Friction ridge impressions consist of ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis, or skin. The data represented in friction ridge impressions allow a determination that corresponding areas of friction ridge impressions either originated from the same source or were not made by the same source. (See figure B-1 on page B-2 for an example of a collected fingerprint.)

B-4. (U) The following are required for proper collection of a fingerprint:

- Ensure the subject's fingers and collection surface are clean prior to collecting fingerprints. Excessive dirt, grease, and/or dryness of the print area will likely result in an unreadable fingerprint capture.
- Ensure the biometric collection system is clean before collecting fingerprints. For example, make sure the fingerprint silicone membrane on the tactical handheld biometric collection device is clean by applying a small piece of clear tape to the silicone membrane to lift residual fingerprint images, dirt, oils, and other debris.
- The collector should maintain control of subject's finger, to include slight and consistent pressure for a slap or rolled fingerprint.

B-5. (U) For collecting rolled fingerprints, roll a subject's finger from knuckle to knuckle and nail to nail (from 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 are collected whenever possible.

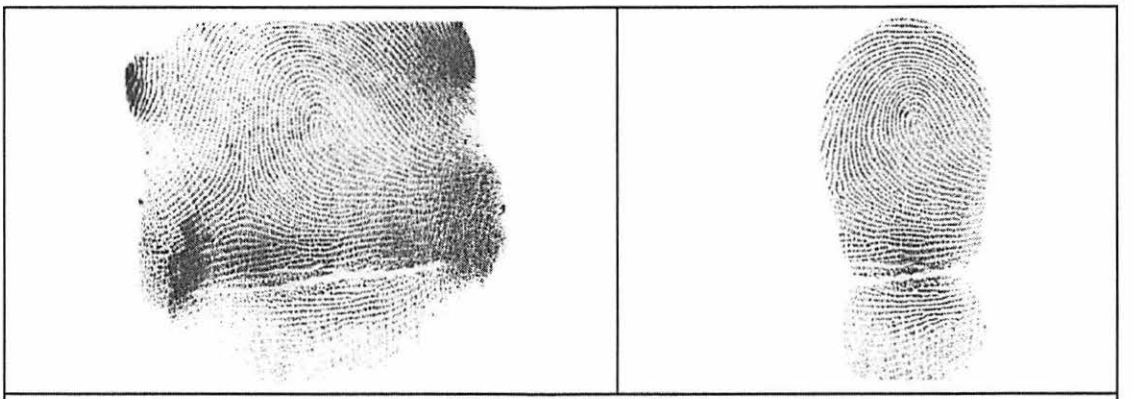


Figure B-1. (U) Example of a collected fingerprint

PALM PRINTS (U)

B-6. (U) A palm print uses the physical structure of an individual's hand for recognition. A palm print consists of a knife (writer) edge and front edge. The knife edge is from the wrist bone to the tip of the pinkie. The front edge is from the wrist along the thumb line to the tip of the index finger.

B-7. (U) Palm prints are derived from the patterns presented in a friction ridge impression. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. Palm prints can be collected as rolled ink-on-card, scanned live, collected from intentional palm prints (such as, inked prints in financial ledgers), or lifted from surfaces touched by an individual (latent palm prints).

B-8. (U) Palm print recognition implements many of the same matching characteristics that have allowed fingerprint recognition to be one of the most well-known and best publicized biometric techniques. However, this technique is not as advanced as fingerprint recognition and has shortcomings associated with its newness. Specifically:

- Palm recognition is slower than fingerprint recognition, due to restraints in computing capabilities and live-scan technologies.
- Palm print applications are hampered by the lack of a current baseline. The collection and storage of palm prints of sufficient quality will yield more palm print matches within automated systems.
- Error rates are decreased when comparing live-scan enrollment data with live-scan data. Improvements in matches between live-scan and latent print data are still needed.

IRIS IMAGES (U)

B-9. (U) Having only become automated and available within the past decade, the iris recognition concept and industry are still relatively new. The iris is the colored portion of the eye and is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. The coloring is based on the amount of melatonin pigment within the muscle. Irises are unique and structurally distinct, which allows them to be used for recognition purposes.

B-10. (U) Iris recognition is the process of identifying an individual by analyzing the random patterns of the iris. The following are iris image collection and system considerations:

- Iris identification systems use near infrared light to illuminate the iris.
- Iris recognition is most useful when verifying the identity of a previously enrolled individual. Iris image verification is the most accurate means of biometrically confirming an individual's identity at this time.

- During iris image collection, the individual's head should is in a stabilized position to prevent movement. All obstructions are removed from the individual's iris area, to include glasses, contact lenses, eyelashes, and hair. The captured image shows the iris and pupil to the maximum extent possible with no glare obscuring any part of the iris. (See figure B-2 for proper iris image alignment.)
- Iris images are collected from deceased individuals; however, collecting up to 30 minutes post mortem is optimal. Environmental conditions can hinder this timeline and render the irises unreadable, so iris images should be collected as soon as practical.

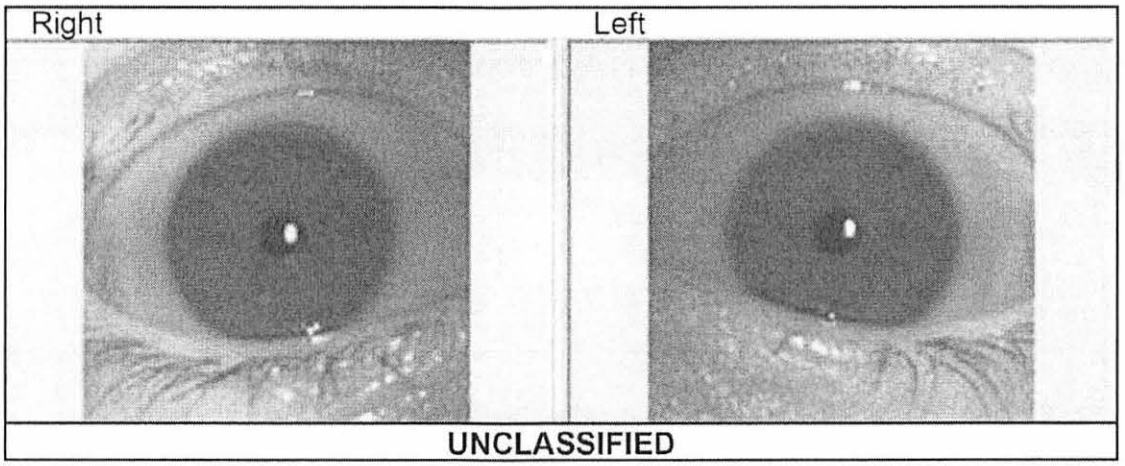


Figure B-2. (U) Proper iris image alignment

FACIAL IMAGES (U)

B-11. (U) Humans instinctively use faces to recognize individuals. Automated facial recognition systems can be used for both verification and identification of an individual. Automated facial recognition is the process of submitting an image collected (through various means) into a repository of other facial images for an algorithm-based search and potential match. Early automated facial recognition algorithms used simple geometric models, but advancements in computing capabilities over the last decade now enable the database to produce more refined candidates with greater computing speeds and accuracy. Major advancements and initiatives in the past 10 to 15 years have propelled facial recognition technology into the forefront; however, the technology does not render 100 percent automated matching.

B-12. (U) Unlike fingerprint and iris recognition, automated facial recognition is not standardized. There are a number of algorithms currently used by different agencies throughout the intelligence community.

B-13. (U) The success of automated facial recognition relies on the quality of the images submitted into the database for searching. Accuracy is affected by several factors: the quality of the image, pose, and angle of the individual in the image, obstructions (such as hats, sunglasses, or hair), illumination, shadowing and facial hair.

B-14. (U) The following are elements critical in the collection of facial images and for automated searching:

- A straight forward, well-lit, neutral background free of distracting objects (such as personnel and equipment).
- The individual being photographed should remove glasses, sunglasses, or other items obscuring the facial area.
- The facial image should include the top of the head to the bottom of the neck, including the ears.
- The facial image should be expressionless.

- The image environment should have sufficient lighting. Improper lighting creates shadows, and direct light creates overexposure.
- The capture device should be level and aligned with the subject's face to ensure a high-quality photograph. Generally, the camera lens is level at subject's nose height to prevent distortion.
- Profile pictures (left and right facial capture) should be captured in the same manner as above. (See figure B-3 for proper facial image alignment.)

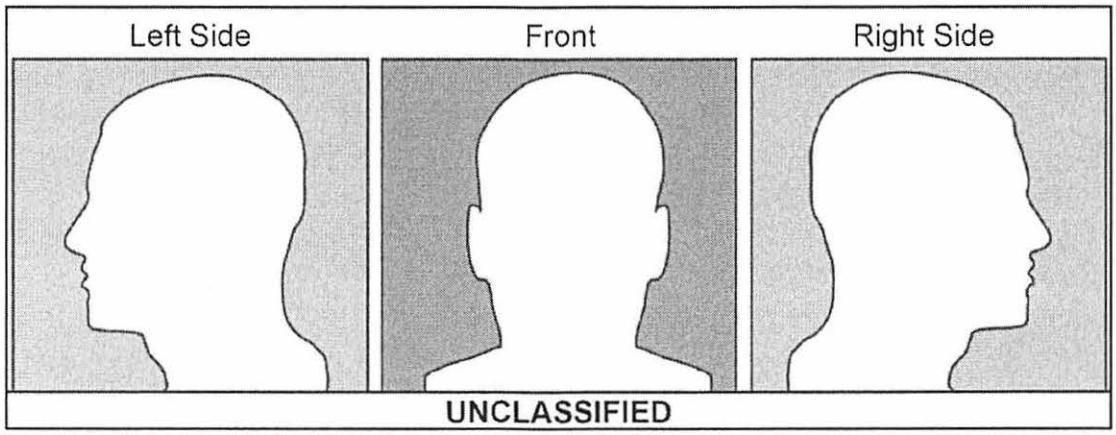


Figure B-3. (U) Proper facial alignment

DNA PROFILES (U)

B-15. (U) DNA is inherited from both the mother and the father. There are two types of DNA, nuclear and mitochondrial. Nuclear DNA is found in the nucleus of the cell and is the more accurate of the two types. Mitochondrial DNA is inherited only from the mother, so it is not used as a means of identification in any DOD database. Nuclear DNA can be more easily acquired in blood, semen, saliva, and skin cells. Although 99.9 percent of human DNA sequences are the same in every person, enough of the DNA is different to distinguish one individual from another. The following items can be swabbed for nuclear DNA sampling:

- Cigarette butts.
- Shirt collars.
- Hats.
- Weapons.
- Bottles.
- Envelopes.

B-16. (U) DNA is very sensitive to contamination. Secure the collected DNA sample in a clean, sterile container immediately after collection. To ensure proper DNA collection, the following is required:

- The collector should wear latex gloves to avoid direct or indirect contact with the sample. The collector should not let samples come in contact with each other.
- The collector uses a DNA swab to collect a sample from the subject's inner cheek or other source of bodily fluids (blood). Use only one swab per person. If swabbing the cheek, the collector ensures the swab is in contact with the sample area for approximately 15 seconds.
- The collector does not remove limbs or body pieces when collecting DNA from the deceased, Instead, the collector collects a DNA sample from an uncontaminated area or source.
- The collector puts the evidence into a clean paper bag or envelope. The collector avoids putting the sample into a plastic bag to prevent degradation from moisture. The collector puts only one sample per container to avoid cross-contamination of samples.
- The collector ensures samples are associated with a specific individual (name, global unique identifier, electronic fingerprint transaction, or individual tracking number). (See figure B-4 for DNA swab examples.)

B-17. (U) After collection, DNA is submitted to a laboratory for analysis. DNA is highly accurate in person of interest identification and linking individuals to a location, event or device.

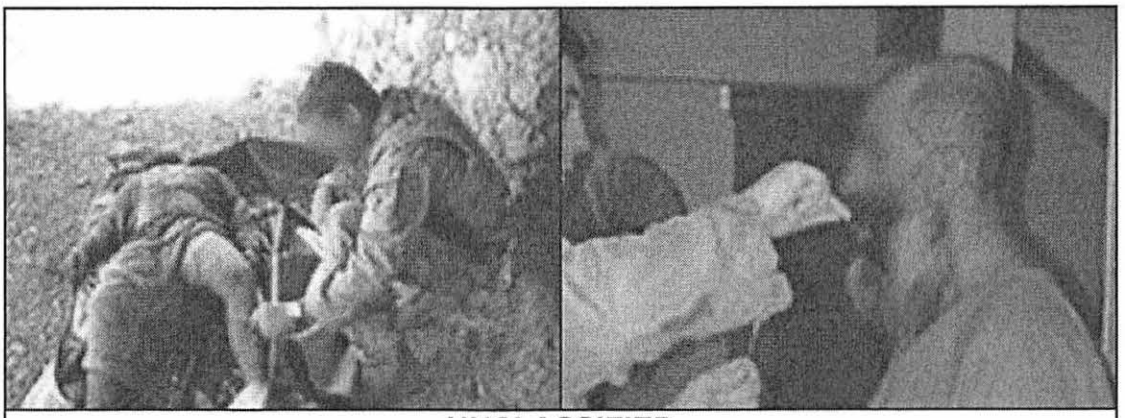


Figure B-4. (U) DNA swab examples

VOICE (U)

B-18. (U) Voice recognition uses the physical structure of an individual's vocal tract and the individual's behavioral characteristics. The peculiarities of an individual's voice can be isolated and thereby differentiated from all other voice patterns, modulations, pitch, and other measurable characteristics. Analysis occurs on a model in which changes over time are monitored, which is similar to other behavioral biometric modalities, such as dynamic signature, gait, and keystroke recognition. This modality is best for one-to-one comparison versus one-to-many, and is still evolving.

THE WAY AHEAD (U)

B-19. (U) Army requirements, commander evaluations, and other factors will help determine what biometric and forensic capabilities are present during future operations. As analysts are able to more quickly and accurately analyze and transmit biometric data, the biometric processes will need to be refined to better support commanders at all levels and in all operational environments.

RELIABILITY AND ACCURACY (U)

B-20. (U) The reliability and accuracy of biometric modalities depend on various factors. The most significant factors are human error in the collection and exploitation of biometric samples and the quality of the biometric samples collected.

B-21. (U) The accuracy of biometric systems depends on the threshold scores established within each system and is affected by several factors. These factors include—

- Sample quality.
- Algorithms in use.
- Acceptable false-alarm rate.
- Repository size (number of samples to which the biometric sample is compared).

B-22. (U) Some common mistakes are—

- Swapped or duplicate fingers between the left and right hand sections of the card.
- Swapped hands when referencing the flat four slaps versus the individual rolled fingers.
- Flat finger captured without proper technique.
- Flat four images captured without all the fingers present.
- Rolled fingers that are lifted prematurely.

- Facial images marked as frontal pose that are not frontal pose.
- Iris images captured with bad technique (that is, shadow or mirrored eyes).

B-23. (U) Many of the current DOD systems are multimodal. This allows collection of multimodal biometrics, which increases the accuracy of a comparison. Although this method is more time-consuming, multimodal biometrics achieves a highly reliable biometric authentication.

Appendix C

Biometrically Enabled Watch List Categories (Tiers) (U)

(U) Historically, watch lists have been name-based, and the success or failure of the watch list rested on a human screener's ability to determine the identity of the person encountered. Enemies, adversaries, and even neutral personnel have a stake in hiding their identities by using disguises, aliases, and falsified documents. Using such means, they have been successful at fooling the human screeners. Improved biometric collection, matching capabilities, and better analysis at all levels of intelligence increases the effectiveness of watch lists by turning positive identification into an exercise of automated biometric recognition.

C-1. (U) Each BEWL tier comprises persons of interest—each identified by a reference number—for whom a specific action is recommended. The composition of the tiers is determined by the level or nature of the threat the person of interest poses to U.S. and friendly forces. The tier or category criteria also stipulate the actions permissible by the unit's authorities, missions and existing rules of engagement, or the terms of the controlling security or status-of-forces agreement. BEWL tiers listed in figure C-1 on page C-2 are examples of those currently in use in counterinsurgency operations and may change as commanders deem necessary.

C-2. (U) When the DOD BEWL is developed for use in all combatant command areas of responsibility, it does not contain action recommendations due to the number and variety of rules of engagement and authority limitations. Instead, the DOD BEWL categorizes persons of interest according to biometrics-community-accepted terminology. This terminology describes a person's past known behavior and other characteristics (for example, IED maker, resident of a particular city, member of a particular group, or leader of a specific unit). The action-based tier system continues at the combatant command level and below. Figure C-2 on page C-3 shows examples of DOD-level common categories and subcategories.

C-3. (U) The current DOD-level categorical watch list consists of—

- Forty-seven categories and 71 subcategories.
- Specific alert categories that can be assigned based on known or assessed data unique to an identity.
- Greater specificity for the operator at the point of encounter.

Tier	*Official guidance*	*Who qualifies*
1	**Detain if encountered.** Subject is deemed a significant threat to multinational partners or is of high intelligence value.	Only targets vetted by Headquarters, Joint Task Force X-XX, are nominated to watch list tier 1.
2	**Question or detain if encountered.** Subject is wanted for questioning and may be a threat to multinational partners. On-scene commander will request reason for this tier from the unit intelligence staff and make decision to tactically question or detain.	• All multinational force targets with previous biometric enrollments. • Counterintelligence individuals of interest. • Local commanders' individuals of interest. • Subjects biometrically linked to insurgent activities.
3	**Assess** Prepare tracking report.	Person of interest.
4	**Don't hire/Deny access/Disqualify for training.** Denies all U.S. benefits, including access to U.S. installations or training by U.S. forces. Subject has at one time been deemed a potential threat to U.S. forces or multinational partners.	• All individuals who have been previously detained by multinational forces at any time, for any reason. • Individuals fired from U.S. installations for intelligence-related or antimultinational force activities.
5	**Deny base access.** Designed to deny base access to U.S. installations and facilities.	All individuals who have been fired from U.S. installations for misconduct, criminal behavior (such as, drugs or theft), or contagious diseases.
6	**Track movement.** Track individuals of interest without negative bias or hindering movement.	Individuals in the wrong place at the wrong time (that is, nonparticipant objective encounters, subjects enrolled near improvised explosive device incidents, associates of known insurgents).
UNCLASSIFIED		

Figure C-1. (U) Biometrically enabled watch list tiers example

Category	*Subcategory*	*Alert*
Person of interest—Department of Defense	Suspicious activity	This individual has been assessed as a Department of Defense person of interest.
Former detainee—Other, Operation Iraqi Freedom/ Operation Enduring Freedom	Wanted—escapee	This individual is a former detainee in the Afghanistan or Iraq theater of operations.
Known or suspected terrorist	Insurgent or terrorist affiliation—Taliban	This individual has met the threshold and is assessed to be a known or suspected terrorist by the Federal Bureau of Investigation terrorist screening center.
National security threat	Insurgent or terrorist affiliation—[name of affiliated group]	This individual has been assessed to be a potential national security threat by the Defense Counterterrorist Center.
Insurgency/Terrorism	Insurgent/terrorist affiliation—[name of affiliated group]	There are indicators this person could have previously been involved in insurgent or terrorist activity.
Piracy	Piracy—Somalia	This individual should be questioned concerning his or her biometric association with piracy.
Suspected facilitator	Insurgency facilitator	This individual is a suspected insurgent facilitator.
Criminal Activity/ Misconduct	Criminal—drug related	There are indicators this person could have been involved previously in criminal activity or misconduct.
Foreign intelligence entity threat	Failed counterintelligence screening	There are indicators this person could pose a force protection threat.
UNCLASSIFIED		

Figure C-2. (U) DOD-level category and subcategory examples

This page intentionally left blank.

Glossary (U)

(U) The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ATP 2-22.82 is the proponent are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition. Refer to the *Common Biometric Vocabulary*, published by the Defense Forensic and Biometrics Agency, for additional definitions. All acronyms and their full forms are unclassified.

SECTION I – ACRONYMS AND ABBREVIATIONS (U)

ABIS	Department of Defense Automated Biometric Identification System
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AR	Army regulation
ATP	Army techniques publication
BAT-A	Biometrics Automated Toolset–Army
BEI	biometrics-enabled intelligence
BEWL	biometrically enabled watch list
BI2R	Biometric Identity Intelligence Resource
BIAR	biometric intelligence analysis report
BLIIP	biometrically linked identity intelligence profile
COIST	company intelligence support team
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOMEX	document and media exploitation
EO	executive order
FBI	Federal Bureau of Investigation
F3EAD	find, fix, finish, exploit, analyze, and disseminate
FEI	forensic-enabled intelligence
FM	field manual
HUMINT	human intelligence
IDENT	Department of Homeland Security Automated Biometric Identification System
IED	improvised explosive device
Interpol	International Criminal Police Organization
IPB	intelligence preparation of the battlefield
JP	joint publication

JWICS	Joint Worldwide Intelligence Communications System
MCRP	Marine Corps reference publication
MCWP	Marine Corps warfighting publication
MDMP	military decision making process
NIPRNET	Nonsecure Internet Protocol Router Network
PED	processing, exploitation, and dissemination
S-2	battalion or brigade intelligence staff officer
SGT	sergeant
SIPRNET	SECRET Internet Protocol Router Network
TECHINT	technical intelligence
TC	training circular
U.S.	United States

SECTION II – TERMS (U)

associated data (U)

(U) Physical and nonphysical attributes of an individual from whom the biometric sample has been collected. Also called biographical characteristics.

authoritative source (U)

(U) A Department-of-Defense-approved repository of biometric information.

behavioral characteristic (U)

(U) An attribute that can be learned or acquired over time, rather than one based primarily on biology.

biographical characteristic (U)

(U) See associated data.

biological characteristic (U)

(U) An individual attribute based primarily on an anatomical or physiological characteristic, rather than a learned behavior.

biometric (U)

(U) A measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual.

biometrically enabled watch list (U)

(U) Any list of persons of interest with individuals identified by biometric sample or the sample's unique identification number instead of by name, and the desired or recommended disposition instructions for each individual.

biometric data (U)

(U) Computer data about an individual created by biometric systems during an enrollment, verification, or identification process.

biometric file (U)

(U) The standardized individual data set resulting from one or more biometric enrollments.

biometric identification (U)

(U) 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.

biometric modality (U)

(U) A type or class of biometric sample originating from a person.

biometrics (U)

(U) (joint) The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

biometric sample (U)

(U) Data representing a biological characteristic of a person as captured by a biometric system.

***biometrics-enabled intelligence (U)**

(U) (Army) Intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements.

biometric system (U)

(U) A grouping of multiple individual components (such as a sensor, matching algorithm, and result display) combined to perform a task related to collecting or supporting analysis of biometric data.

biometric verification (U)

(U) The automated process of comparing a submitted biometric sample against one biometric file (one-to-one) to determine if they match. Also called biometric authentication.

contextual data (U)

(U) Elements of biographical characteristics and situational information (who, what, when, where, why, how) associated with an enrollment.

intelligence operations (U)

(U) (Army) The tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements. (ADRP 2-0)

local trusted source (U)

(U) A subset of an authoritative source that is established at the operational level to accomplish a specific function in support of a mission.

local untrusted source (U)

(U) A local repository of biometric files that have not been enrolled with an authoritative or local trusted source.

warning intelligence (U)

(U) (joint) Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0)

This page intentionally left blank.

References (U)

REQUIRED PUBLICATIONS (U)

(U) These documents must be available to intended users of this publication.

(U) Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

(U) Most Army doctrinal publications are available online: www.apd.army.mil.

(U) ADRP 1-02. *Terms and Military Symbols*. 2 February 2015.

(U) JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

RELATED PUBLICATIONS (U)

(U) These documents are cited in this publication.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS (U)

(U) Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

(U) Most DOD publications are available at the DOD Issuances Web site: www.dtic.mil/whs/directives.

(U) DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*. 7 December 1982.

(U) DODD 3025.18. *Defense Support of Civil Authorities (DSCA)*. 29 December 2010.

(U) DODD 8521.01E. *Department of Defense Biometrics*. 21 February 2008.

(U) DODI O-3300.04. *Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)*. 25 May 2012.

(U) DODI C-5240.08. *Counterintelligence (CI) Security Classification Guide*. 28 November 2011. This classified publication is available online at The DOD Issuances Web page (SIPRNET): www.dtic.smil.mil/whs/directives/corres/ ins1.html. Accessed 23 September 2015.

(U) JP 2-0. *Joint Intelligence*. 22 October 2013.

(U) JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

(U) JP 3-0. *Joint Operations*. 11 August 2011.

ARMY PUBLICATIONS (U)

(U) Most Army doctrinal publications are available online: www.apd.army.mil.

(U) ADP 5-0. *The Operations Process*. 17 May 2012.

(U) ADRP 1-03. *The Army Universal Task List*. 2 October 2015.

(U) ADRP 2-0. *Intelligence*. 31 August 2012.

(U) ADRP 3-28. *Defense Support of Civil Authorities*. 14 June 2013.

(U) ADRP 3-37 (FM 3-37). *Protection*. 31 August 2012.

(U) ADRP 3-90. *Offense and Defense*. 31 August 2012.

(U) ADRP 5-0. *The Operations Process*. 17 May 2012.

(U) AR 25-55. *The Department of the Army Freedom of Information Act Program*. 1 November 1997.

(U) AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

(U) AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

(U) ATP 2-01. *Plan Requirements and Assess Collection*. 19 August 2014.

(U) ATP 2-01.3/MCRP 2-3A. *Intelligence Preparation of the Battlefield/Battlespace.* 10 November 2014.

(U) ATP 2-22.4. *Technical Intelligence.* 4 November 2013.

(U) ATP 2-33.4. *Intelligence Analysis.* 18 August 2014.

(U) ATP 2-91.7. *Intelligence Support to Defense Support of Civil Authorities.* 29 June 2015.

(U) ATP 2-91.8. *Techniques for Document and Media Exploitation.* 5 May 2015.

(U) ATP 3-60 (FM 3-60). *Targeting.* 7 May 2015. (U)

FM 2-0. *Intelligence Operations.* 15 April 2014. (U)

FM 2-22.2. *Counterintelligence.* 21 October 2009.

(U) FM 3-21.10. *The Infantry Rifle Company.* 27 July 2006.

(U) FM 3-50. *Army Personnel Recovery.* 2 September 2014.

(U) FM 3-53. *Military Information Support Operations.* 4 January 2013.

(U) FM 3-55. *Information Collection.* 3 May 2013.

(U) FM 3-63 (FM 3-39.40). *Detainee Operations.* 28 April 2104.

(U) FM 3-90-1. *Offense and Defense Volume 1.* 22 March 2013.

(U) FM 3-90-2. *Reconnaissance, Security, and Tactical Enabling Tasks Volume 2.* 22 March 2013.

(U) FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

(U) FM 27-10. *The Law of Land Warfare.* 18 July 1956.

OTHER PUBLICATIONS (U)

(U) *Common Biometric Vocabulary.* DOD Biometrics and Forensics Agency. April 2013. Available online at the Defense Forensics and Biometrics Agency Web site at http://www.biometrics.dod.mil. Select Common Biometric Vocabulary from the References drop-down menu. Accessed 10 September 2015.

(U) Department of Defense Biometrics Security Classification Guide. No date. This publication is marked For Official Use Only and is available online at the Intelligence Knowledge Network Web site: https://ikn.army.mil. Select "MI Active Doctrine Page" from the Resources drop-down menu. Accessed 10 September 2015.

(U) *Electronic Biometric Transmission Specification.* Version 3.0. 8 December 2011. Available online at the Defense Forensics and Biometrics Agency Web site at http://www.biometrics.dod.mil/. Select Standards Publications from the References drop-down menu. Accessed 17 August 2015.

(U) EO 12333. *United States Intelligence Activities.* 4 December 1981. Available online at the National Archives Federal Register Web site at http://www.archives.gov/federal-register/codification/executive-order/12333.html. Accessed 17 August 2015.

(U) Privacy Act of 1974 (Section 552a, Title 5, Unites States Code). Available online at http://uscode.house.gov. Use the Popular Name Tool on the left side of the Web page. Accessed 17 August 2015.

(U) Title 32, United States Code. National Guard. Available online at http://uscode.house.gov. Accessed 11 September 2015.

(U) Title 50, United States Code. War and National Defense. Available online at http://uscode.house.gov. Accessed 11 September 2015.

RECOMMENDED READINGS (U)

(U) These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS (U)

(U) Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

(U) Most DOD publications are available at the DOD Issuances Web site: www.dtic.mil/whs/directives.

(U) DODD 1000.25. *DOD Personnel Identity Protection (PIP) Program.* 19 July 2004.

(U) DODD 2310.01E. *DOD Detainee Program.* 19 August 2014.

(U) DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning.* 11 October 2012.

(U) DODD 5200.27. *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.* 7 January 1980.

(U) DODD 5240.01. *DOD Intelligence Activities.* 27 August 2007.

(U) JP 1. *Doctrine for the Armed Forces of the United States.* 25 March 2013.

(U) JP 3-05. *Special Operations.* 16 July 2014.

(U) JP 3-13.1. *Electronic Warfare.* 08 February 2012.

(U) JP 3-24. *Counterinsurgency.* 22 November 2013.

(U) JP 3-28. *Defense Support of Civil Authorities.* 31 July 2013.

(U) JP 3-60. *Joint Targeting.* 31 January 2013.

(U) JP 5-0. *Joint Operation Planning.* 11 August 2011.

ARMY PUBLICATIONS (U)

(U) Most Army doctrinal publications are available online: www.apd.army.mil.

(U) ADP 2-0. *Intelligence.* 31 August 2012.

(U) ADP 3-0. *Unified Land Operations.* 10 October 2011.

(U) ADRP 3-0. *Unified Land Operations.* 16 May 2012.

(U) AR 380-13. *Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations.* 30 September 1974.

(U) ATP 2-19.4. *Brigade Combat Team Intelligence Techniques.* 10 February 2015. ATP 2-19.4 includes COIST employment techniques.

(U) ATP 2-22.85. *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations.* 1 April 2014.

(U) ATP 3-90.15. *Site Exploitation Operations.* 28 July 2015.

(U) FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection.* 10 October 2007.

OTHER PUBLICATIONS (U)

(U) *Capturing Legible Fingerprints.* Federal Bureau of Investigation. January 2013. Available online at Federal Bureau of Investigation Web site at http://www.fbi.gov/hq/cjisd/takingfps.html. Accessed 18 August 2015.

(U) *DOD Capstone Concept of Operations for Employing Biometrics in Military Operations.* 10 June 2012. Available online at the Defense Forensics and Biometrics Agency Web site at http://www.biometrics.dod.mil. Select the Collaboration drop-down menu. Accessed 3 September 2015.

(U) National Security Presidential Directive/NSPD-59/Homeland Security Presidential Directive HSPD-24. *Biometrics for Identification and Screening to Enhance National Security.* 5 June 2008. Available online at the Government Printing Office Web site at http://www.gpo.gov/fdsys/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf. Accessed 20 August 2015.

WEB SITES (U)

(U) See appendix A for Web sites listed by network and topic.

PRESCRIBED FORMS (U)

(U) This section contains no entries.

REFERENCED FORMS (U)

(U) Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site: www.apd.army.mil.

(U) DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

Index (U)

(U) Entries are by paragraph number unless indicated otherwise.

(U) Entries are by paragraph number unless indicated otherwise.

(U) Entries are by paragraph number unless indicated otherwise.

(U) Entries are by paragraph number unless indicated otherwise.

By Order of the Secretary of the Army:

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

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1529501

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

Freedom of Information/
Privacy Office

FEB 2 8 2020

Mr. Steven Aftergood
1120 16th Street NW
Suite 400
Washington, DC 20036

Dear Mr. Aftergood:

This is in further response to your Freedom of Information Act (FOIA) request of November 10, 2015 requesting a copy of ATP 2-22.82 on Biometrics-Enabled Intelligence and supplements our letter of November 20, 2019.

Coordination has been completed with another element of our command and records were returned to this office for our review and direct response to you.

We completed a review of the documents. As a result of our review, information has been sanitized pursuant to Title 5 U.S.Code 552 § (b)(3) of the FOIA, which applies to information that is exempt by statute. The statute invoked under (b)(3) is 50 U.S. Code § 3024(i), which allows for the protection of intelligence sources and methods.

The withholding of the information described above is a partial denial of your request. This denial is made on behalf of Major General Gary W. Johnston, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the FOIA. You have the right to appeal this decision to the Secretary of the Army. Your appeal must be postmarked no later than 90 calendar days from the date of this letter. After the 90-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis of your disagreement with the response and provide justification for a reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office, for forwarding, as appropriate to the Secretary of the Army, Office of the General Counsel.

Commander
U.S. Army Intelligence and Security Command (APPEAL)
Freedom of Information/Privacy Office
2600 Ernie Pyle Street
Suite 3S02-B
Fort George G. Meade, Maryland 20755-5995

There are no assessable FOIA fees for the processing of this request.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651, or email the INSCOM FOIA office at: usarmy.meade.902-mi-grp.mbx.inscom-foia-service-center@mail.mil and refer to case #0070F-20. Please note that you now have the ability to check the status of your request online via the U.S. Army Records Management and Declassification Agency (RMDA) website: https://www.foia.army.mil/FACTS/CaseStatus.aspx. Please refer to FOIA Control Number: FP-20-003263. If you have any questions or wish to discuss reformulation or an alternative time frame for the processing of your request, you may contact our FOIA Public Liaison, Mrs. Joanne Benear, for any further assistance and to discuss any aspect of your request at 301-677-7856. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, email at ogis@nara.gov, telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Michael T. Heaton
Director
Freedom of Information/Privacy Office
Investigative Records Repository

Enclosure