



HANDBOOK



No. 11-25

APR 11



Commander's Guide to Biometrics in Afghanistan



Observations, Insights, and Lessons

U.S. UNCLASSIFIED//FOR OFFICIAL USE ONLY
REL NATO, GCTF, ISAF, ABCA
EXEMPT FROM MANDATORY DISCLOSURE under FOIA Exemptions 2 and 5

Handling Instructions for CALL Electronic Media and Paper Products

Center for Army Lessons Learned (CALL) authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S., coalition, and allied efforts.

The information contained in this product reflects the actions of units in the field and may not necessarily be approved U.S. Army policy or doctrine.

This product is designed for official use by U.S., coalition, and allied personnel and cannot be released to the public without the expressed written consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulation (AR) 380-5, section 5-2.

Official military and civil service/government personnel, to include all coalition and allied partners, may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official products or research. However, integration of CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels and cannot be released to the public without the expressed written consent of CALL.

This product may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military and government officials have access to these products.

Regulations strictly forbid posting CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Department of Defense (DOD) websites that do not restrict access to authorized personnel. AR-25-1, 15 Jul 2005, Army Knowledge Management and Information Technology, paragraph 6-4 n (2) (b) and DOD Web Site Administration Policy and Procedures (11 Jan 2002), Part II, paragraph 3.6.1 require appropriate mechanisms to protect sensitive information.

When no longer needed, all CALL "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CDROM destroyers.

To allied and coalition personnel:

This information is furnished with the understanding that it is to be used for defense purposes only, that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States, and that it is not to be revealed to another country or international organization without the written consent of CALL.



Foreword

Biometrics is a decisive battlefield capability being used with increasing intensity and success across Afghanistan. It effectively identifies insurgents, verifies local and third-country nationals accessing our bases and facilities, and links people to events. The biometric technology allows the targeting of persons of interest (POIs) more precisely and helps to provide desperately needed security for local populations. Across Afghanistan, there are normally four to five watch-list hits each day based solely on biometrics. These watch-list hits allow the identification and potential detainment of POIs who operate counter to Afghan, International Security Assistance Force (ISAF), and coalition goals. Beyond Afghanistan, biometrics enables the tracking of POIs across international borders and prevents them from entering the United States.

Throughout the Afghan government, Afghan leaders are embracing biometrics not only to defeat insurgents and identify criminals, but also to verify its lawful citizens. In partnership with the Afghan Ministry of Interior, the coalition is employing 1,000 Afghan citizens to conduct biometric enrollments of the Afghan population in a program that will support the Afghan national identification card. Over the next two years, these enrollers will operate in every province, district, border port of entry, and major airport in Afghanistan. These efforts will improve security and enable the potential provision of numerous government services. Our Afghan partners also have achieved convictions in the Afghan court system based solely on biometric and forensic data.

As leaders, we are responsible for operating in the most effective way possible while protecting our subordinates from harm — biometrics is a decisive capability that allows us to do both simultaneously. Almost every operation provides us the opportunity to collect biometrics; the more enrollments contained in the database the more likely POIs will be identified. As a result, battlefield effectiveness will increase, our troops will be safer, and the Afghan populace will be protected in greater measure.

The use of biometrics on the battlefield is relatively new. There is no formal doctrine; universally accepted tactics, techniques, and procedures; or institutionalized training programs across the Department of Defense. To help bridge that gap, the Center for Army Lessons Learned produced this handbook to help guide commanders' employment of biometric capabilities in Afghanistan. This handbook contains valuable information to aid unit leaders preparing for and conducting biometrics collection activities allowing ISAF, coalition, and U.S. forces to maximize the effects of this critical capability.

My thanks to those who have contributed to this document. Your willingness to invest your time, along with your candor and insight, made this publication possible.



ROBERT S. HARWARD
Vice Admiral, U.S. Navy
Commander, Combined Joint Interagency
Task Force 435

Commander's Guide to Biometrics in Afghanistan	
Table of Contents	
Introduction	1
Chapter 1. Operationalizing Biometrics	3
Chapter 2. Afghan Theater Overview: Impact on Biometrics	13
Chapter 3. Leader Responsibilities	17
Chapter 4. Biometrics Support to Operations	27
Chapter 5. Biometrics-Enabled Intelligence	37
Appendix A. Basic Biometric Principles	45
Appendix B. Training	51
Appendix C. Biometrics Systems Architecture	61
Appendix D. Biometrics Glossary	63
Appendix E. Biometric References	79
Appendix F. Special Operations Biometrics	81
Appendix G. CALL Lesson of the Day: Kandahar Biometric Data Collection	85

Center For Army Lessons Learned	
Director	COL Thomas H. Roe
Division Chief	Keith Warman
Author	Dennis Branson, CALL Contractor
Editor	Michael Brooks
Graphic Artist	Dan Neal, CALL Contractor

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

Introduction

Biometrics capabilities on the tactical battlefield enable a wide variety of defensive and offensive operations. Biometrics help ensure enemy personnel, criminals, and other undesirable elements are not allowed access to our facilities, hired to provide services, or awarded contracts. Biometrics is used to vet members of the Afghan government and military with whom our forces interact. Unfortunately, biometrics capabilities we put in the hands of Soldiers, Marines, Sailors, and Airmen — and that we ask unit commanders to employ — are relatively recent additions to the list of capabilities our military employs on the battlefield today.

In most cases, biometrics systems are not part of any unit's modified table of organization and equipment, and yet are used in combat by personnel who do not have a formal skill identifier. There is a lack of formal doctrine for employing biometrics capabilities by units and no recognized task, conditions, and standards that can be instituted to ensure these capabilities are employed consistently to maximum effect. Additionally, the vast majority of training conducted in biometrics is focused on equipment operation and not enough emphasis is given to leader training. The result is that units often struggle to employ biometrics capabilities effectively or to maximize its effects across the operational spectrum.

Within Afghanistan, Task Force Biometrics currently deploys personnel at the brigade combat team (BCT) and regional command (RC) levels to work with unit commanders and their staffs to help integrate biometrics more effectively into mission planning and execution. Task Force Biometrics is ready to provide additional training to any member who collects biometrics — including International Security Assistance Force (ISAF) partners. Task Force Biometrics is also the lead organization for all biometrics-enabled intelligence (BEI) actions in theater and currently maintains BEI personnel at the BCT and RC levels to assist intelligence staffs and provide focused input into the theater biometrics enabled watch list (BEWL). BEI personnel at Task Force Biometrics, in concert with continental U.S. intelligence agencies and organizations, has developed a wide variety of products that fuse biometrics information with forensics, terrain analysis, and other forms of intelligence to provide commanders information that helps better direct counterinsurgency (COIN) operations.

This handbook is intended to help bridge the doctrinal gap within the Department of Defense and to provide unit commanders with useful information to effectively employ biometric capabilities in the unique environment and operational conditions of Afghanistan. It is not intended to replace current or future ISAF guidance on the employment of biometrics; its aim is simply to generate a better understanding of how to integrate biometrics into operations before units deploy to combat.

Overview

Chapter 1 describes basic principles and capabilities of biometrics. Commanders with biometrics experience in Iraq must understand environmental differences in Afghanistan.

Chapter 2 describes how restricted terrain, the nature of the coalition, friendly force operational employment, cultural/political factors, and the lack of infrastructure impact the employment of biometrics in Afghanistan.

Chapter 3 describes leader and staff responsibilities when using biometrics in support of tactical operations.

Chapter 4 describes various missions that can and should be enabled by biometrics.

Chapter 5 describes use of biometrics to support both intelligence operations and analysis.

Appendix A is an overview of the fundamental principles of biometrics.

Appendix B describes the current state of biometrics training.

Appendix C is a visual of the Afghanistan biometrics systems architecture.

Appendix D is a glossary of biometric terms.

Appendix E contains references to some of the best biometrics websites.



Appendix F describes special operations employment of biometrics.

Appendix G is a Center for Army Lessons Learned lesson of the day report from enrollment operations in Kandahar.

This handbook includes information on strengths and weaknesses of common types of biometrics systems in use by ISAF elements. This publication provides commanders with an excellent tool to implement the ISAF commander's current COIN guidance.

Chapter 1

Operationalizing Biometrics

Ghazni Gul		
<p style="text-align: center;">29 January 2010</p>  <p>Ghazni Gul was enrolled in the Biometrics Automated Toolset when encountered on the objective of an intelligence driven raid.</p>	<p style="text-align: center;">04 March 2010</p> <div style="background-color: #f8d7da; padding: 2px; margin-bottom: 5px; font-weight: bold; font-size: small;">ON ALERT? YES</div> <p style="font-size: x-small; margin: 0;">WL1 DETAIN HVT-DETAIN IF ENCOUNTERED. Assessed as HIGH THREAT. Contact USFOR-A BMO</p> <p>Ghazni Gul was identified as an International Security Assistance Force headquarters vetted target and was placed on watch list 1 (WL1) (DETAIN IF ENCOUNTERED) of the Afghanistan biometrics watch list.</p>	<p style="text-align: center;">16 March 2010</p>  <p>Ghazni Gul was encountered at Bagram Air Base entry control point 3 while attempting to visit his brother at the detention facility in Parwan (DFIP). He was identified via iris as being on WL1. Task Force Biometrics contacted Task Force Rakkasan, the targeting unit, who sent an element to take ownership of the subject and escort him to the Salerno Field Detention Site. He was subsequently transferred to the DFIP on 25 April 2010.</p>
<p>The use of three biometric modalities: face, fingerprint, and iris, allowed coalition forces to identify, track and exploit this personality and deny him anonymity. In the case of Ghazni Gul, no deliberate operation was required to identify and detain him. Biometrics stopped him without one shot fired.</p>		

Depiction of watch list 1 high-value target detained as a result of biometrics screening. (Note: Named individual “Ghazni Gul” is fictional and used for training purposes only.)

Scenarios, as the one described above, occur with increasing regularity. Biometrics collections and forensic exploitation of improvised explosive devices (IEDs), cache sites, safe houses, and vehicles support the counterinsurgency (COIN) effort by giving commanders additional tools to separate the insurgents from the populace. Biometrics is a critical COIN nonlethal weapon system. (Appendix A contains a comprehensive description of biometrics collection.)

All units will have access to both table top and hand-held biometrics collection equipment like the Biometrics Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE). This equipment helps units conduct biometrics collection for a wide range of missions across the spectrum of operations. Lessons from theater indicate it is vital for commanders to ensure their personnel are adequately trained to effectively operate the equipment. Just as an infantry commander would not rotate duties of manning a machine gun at random, operation of biometric equipment should be a dedicated mission for a designated group of service members. Evidence in theater indicates that dedicated biometric enrollers increase the level of proficiency and enable more thorough

collections. Complete collections create greater chances of finding persons of interest (POIs). Biometrics collection is a nonlethal weapon system feeding operational synchronization metrics.

The results of collection activities are exploited using theater- and national-level biometric databases. However, poorly executed collections may result in an insurgent gaining access to our facilities or personnel in Afghanistan. For example, if a service member only collects six fingerprints using the HIIDE, one of the four missing prints may be the one extracted from a piece of black tape used to construct an IED. Getting the collection right the first time is a critical component to help biometrics-enabled intelligence (BEI) analysts link POIs to an event. Most importantly, quality collection requires leader involvement, training, and daily vigilance.

Simply stated, collecting fingerprints with biometric collection devices has led to the apprehension of bomb makers and emplacers. Photographing individuals in a given area will assist in development of target packages and build a knowledge base of the populace. Collecting irises provides positive identification of an encountered person, greatly improving force protection at all facilities. Biometrics (e.g., fingerprints, iris images, face photos) will positively identify an encountered person and unveil terrorist or criminal activities regardless of paper documents, disguises, or aliases.

Biometrics and Counterinsurgency

Counterinsurgencies have traditionally succeeded when insurgents were physically separated from the populace. In the past, such separation required relocation into protected areas. Today, with biometrics on the battlefield, we can separate insurgents from the populace without moving anyone. Afghan elders or *maliks* are village leaders who are generally interested in protecting their people. When it is demonstrated how biometrics can separate insurgents from their people and make them safer, they will generally be supportive of enrollments (Figure 1-1). By conducting population management patrols and performing quality enrollments, commanders will know who belongs in a particular area of operation, what they do, and exactly who they are.

The probability of identifying those who are tied to criminal or insurgent activity increases as the biometric database grows. Collecting biographic and contextual information builds a knowledge base of who is in the operational area; however, a biometrics collection device stored in a Conex storage container will not identify a single individual on the biometrics enabled watch list (BEWL). Afghanistan becomes more secure as more individuals involved in nefarious activities are identified and removed from the battlefield. As a result, coalition forces and the Afghan population are safer, and the Government of the Islamic Republic of Afghanistan (GIRoA) achieves legitimacy while the insurgents simultaneously become more isolated.



Figure 1-1. Biometrics enrollment in COIN operations

Relationship Between Biometrics and Forensics

The relationship between biometrics and forensics can be explained when you understand their definitions. Biometrics is the measuring and analysis of physical human attributes and forensics is scientific tests or techniques used in connection with the detection of crime or event. The military term “battlefield forensics” is defined as multidisciplinary, scientific processes, capabilities, and technologies used to establish facts that uniquely identify, associate, and link people, places, things, intentions, activities, organizations, and events to each other in support of battlefield activities such as military intelligence, targeting, and identity superiority operations.

Biometric collection devices used by U.S. forces typically collect fingerprints, iris images, and facial images and stores this data into local and national databases. This data then can be searched upon and compared to other collected biometrics and is used primarily for identification or verification of an individual. Fingerprints and DNA are examples of biometrics and can be collected directly from a detained, willing, or deceased individual. U.S. forces use buccal swabs to capture the buccal cells that line the mouth (Figure 1-2) and digital scanners or standard ink cards to capture fingerprints (Figure 1-3).

Using forensic processes such as lifting a latent fingerprint or collecting DNA from materials or evidence found through the examination of IED components after an explosion can result in identifying biometrics. Through exploitation of these types of biometrics, individual identification and possible attribution can be made. Forensics can also be used to conduct chemical or materials analysis of IED components to determine their possible association with other events and individuals and to establish the facts surrounding an incident.

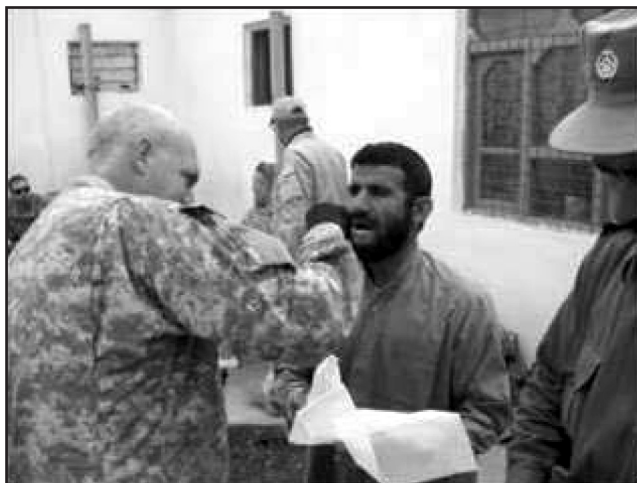


Figure 1-2. Obtaining a buccal swab from an Afghan national



Figure 1-3. Fingerprint enrollment

Specific battlefield forensics are covered in the handbook *Forensics for Commanders*, published by the Office of the Provost Marshal General, and there are a wide variety of forensic activities occurring in Afghanistan today. Many of these activities are conducted specifically for the counter IED effort by individuals from weapons intelligence teams and other related organizations. In addition, units often collect forensics materials during site exploitation missions. IED-related materials are normally exploited by Combined Explosives Exploitation Cell labs, while non-IED materials are handled by the joint expeditionary forensics facility labs. The bottom line is that captured enemy materials and energetic fragments/components must be exploited as quickly as possible and the forensically collected biometrics data transmitted to the authoritative database — Automated Biometrics Identification System (ABIS) (see Figure 1-4).

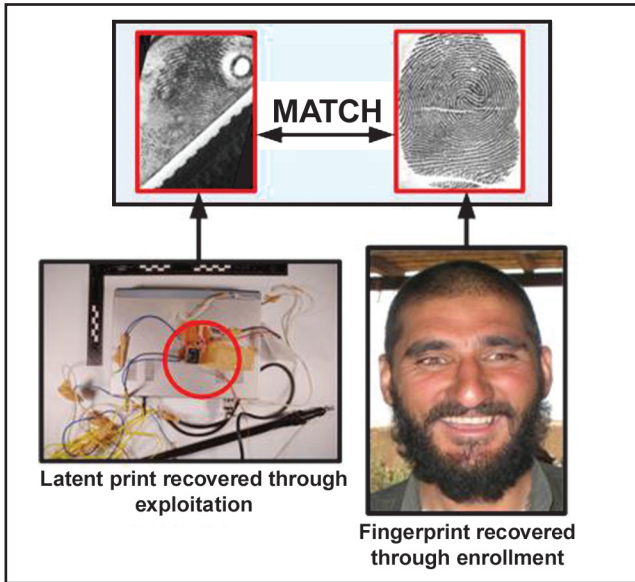


Figure 1-4. ABIS match

In law enforcement, forensic evidence is analyzed to answer questions associated with a case. On the battlefield, forensic materials are analyzed to answer questions associated with intelligence requirements. In a criminal setting, forensic scientists must explain their conclusions to detectives, lawyers, and juries. In a battlefield setting, forensic intelligence analysts must explain their conclusions to commanders, who make decisions about committing forces and conducting specific actions in a combat environment. Forensics on the battlefield in Afghanistan are being used at an increasing rate by the Afghan criminal justice system, and convictions are now occurring in the Afghan courts based solely on biometric evidence. Figure 1-5 depicts the enrollment and exploitation linkage enabled through forensics, analysis, and communication systems.

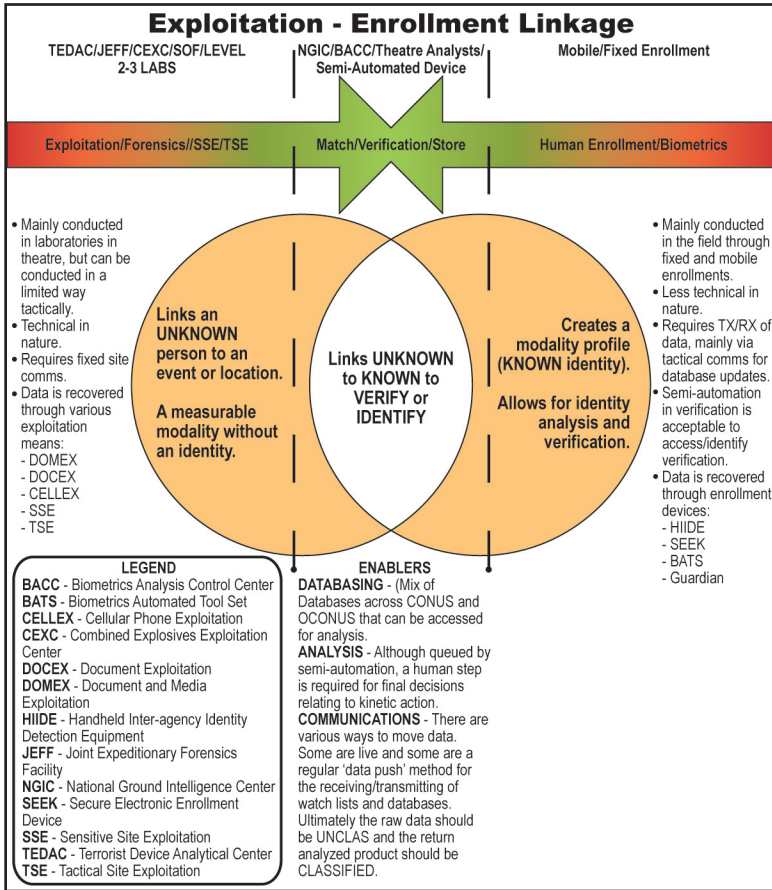


Figure 1-5. Exploitation-enrollment linkage

Biometrics Process

The biometrics process involves collection and transmission of biometrics information to an authoritative database for storage, matching, and sharing to develop the assurance of an individual's identity. It is closely linked to the intelligence process, as the latter determines the significance of the identity revealed by the match (Figure 1-6). The intelligence process is also responsible for the development of a key product used to support tactical biometrics operations — the BEWL. The BEWL, commonly referred to as “the watch list,” is a collection of individuals whose biometrics have been collected and determined by BEI analysts to be threats, potential threats, or who simply merit tracking.

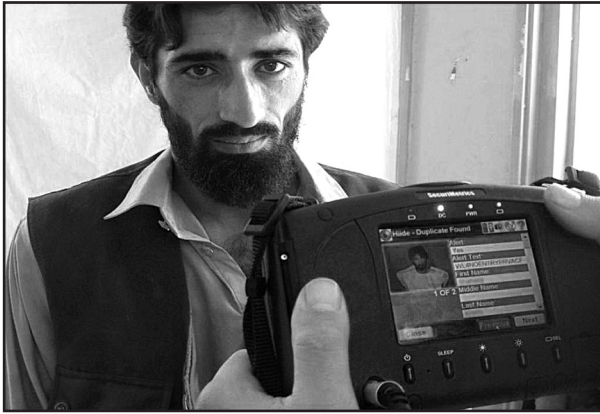


Figure 1-6. HIIDE iris scan

When properly loaded onto a biometrics collection device, the BEWL allows for instantaneous feedback on biometrics collections without the need for real-time communications to the authoritative biometrics database. If the BEWL is not updated on the device though, units may lose their only opportunities to detain a POI. For example, a service member in Helmand province may collect the biometrics of an unidentified male encountered on a combat patrol. If that individual is on the BEWL and the Soldier's HIIDE (Figure 1-7) is properly updated, the Soldier will immediately get the appropriate feedback on what actions to take based on the level of watch list that person is categorized. If the HIIDE has not been properly updated, the unit will have no reason to detain the person of interest and will have lost perhaps its only opportunity to do so.



Figure 1-7. HIIDE kit

If no watch list match is made during a collection, the biometrics data and associated contextual information required for enrollment will be transmitted back to the Department of Defense (DOD) ABIS for matching against all other collected biometrics. If a match is made there, that information is sent to the National Ground Intelligence Center (NGIC) in Charlottesville, VA, which generates a biometrics intelligence analysis report (BIAR) detailing the actions and potential threat of an individual. NGIC then contacts Task Force (TF) Biometrics in Afghanistan which, in turn, contacts the appropriate operational environment owner to provide updated intelligence on the POI. This process can take from a matter of minutes for special operations forces to several days for conventional units if the match is made against a latent fingerprint. Even if no match is made, the biometrics and enrollment information are stored for use in future cases and to enable the BEI process, emphasizing that all collections are important.

Once BEI analysts fuse biometric enrollments, forensic evidence, and all other forms of intelligence they develop the BEWL in cooperation with numerous other intelligence, agencies and organizations. In Afghanistan, regular updates are done by TF Biometrics and posted on secure sites to authorized users. For example, if a watch list level 1 (WL1) or watch list level 2 (WL2) individual is added during the week, TF Biometrics will post snap updates to ensure units minimize the chances of inadvertently releasing a key person of interest. Figure 1-8 graphically depicts the BEWL development, enrollment, and exploitation linkage enabled through forensics, analysis, and communication systems.

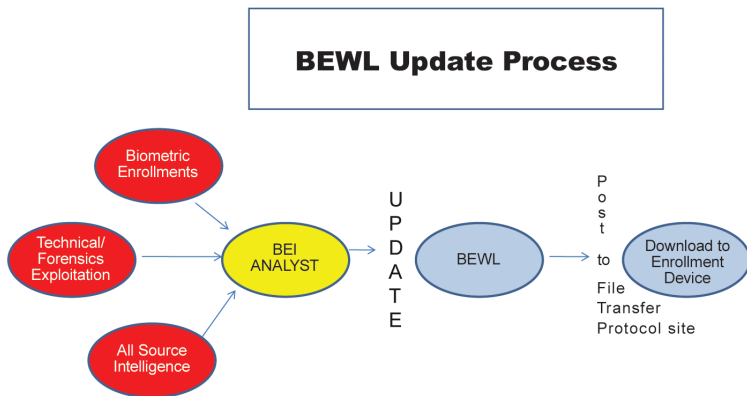


Figure 1-8. BEWL update process

- Twenty-nine BEI analysts are the focal point for the BEWL located throughout the operational environment, including presence at each brigade combat team (BCT).
- Analysts combine biometric modalities, forensic exploitation, and all-source intelligence to develop the BEWL.
- TF Biometrics publishes the BEWL every Sunday; snap updates occur as needed for WL1 or WL2 individuals.
- Units can specifically request to add/delete specific persons on BEWL. Approval for additions are made at the BEI analyst level; deletions require approval from the TF Biometrics director.

Biometrics Value Chain

The Biometrics value chain (Figure 1-9) outlines the biometric process and how each part builds on the next, leading to mission success. The impact of fingerprint collections, both forensically and with biometrics devices, ranges from the battlefield to the U.S. and other areas where we encounter terrorists or insurgents. Through DOD ABIS, fingerprints are matched and shared with the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI). With over 90 million fingerprint entries collected, DHS has the largest database for use in the US-VISIT program, which tracks the entry and exit of foreign visitors by using electronically scanned fingerprints and photographs. The FBI has the largest database of criminal enrollments with over 55 million entries. Through international collaboration, access to other countries' criminal fingerprint enrollments is used to match against collected fingerprints to ensure criminals do not go undetected.

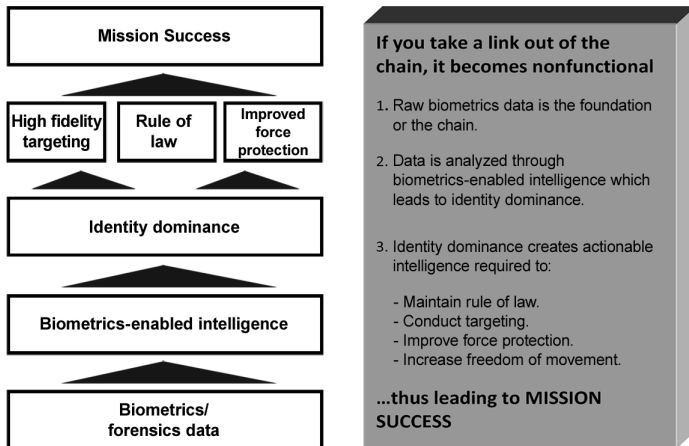


Figure 1-9. Biometrics/forensics value chain

Task Force Biometrics

The organization responsible for fielding, training, and supporting biometric equipment issued to International Security Assistance Force is TF Biometrics. It is headquartered at Camp Phoenix, with subordinate elements located throughout the theater. TF Biometrics trains and equips units to conduct aggressive enrollment missions against specific population sets, such as detainees/prisoners, Afghan National Security Forces (ANSF) personnel, local national hires by coalition forces, and armed contractors, as well as at ports of entry and border crossing points.

TF Biometrics supports development of a biometrics capability for GIROA, to include establishment and operation of an Afghan-owned and operated biometrics database. TF Biometrics works with the North Atlantic Treaty Organization (NATO) training mission to provide equipment, training, and advice to the ANSF, Afghan Ministry of Interior, and other members of the U.S. government. These efforts help generate near-term enrollments, particularly of ANSF personnel, and set the stage for transition of biometrics missions to GIROA. The *Afghan 1,000 Plan* — a local national contract with the U.S. — will establish a foundation of an Afghan biometric enrollment capability enrolling Afghans throughout the country.

TF Biometrics has expanded its ability to support biometrics operations by emplacing biometric staff elements at the regional command (RC) and BCT level. Biometric support elements (BSEs) comprised of military and civilian contractors are located in each RC and assist commanders in implementing biometrics into all operations down to the company level, including mission planning, equipment fielding, technical support, and training.

In summary, Afghanistan presents an extraordinarily complicated environment for the broad employment of biometrics. However, the payoff to U.S. and coalition forces is so great in terms of securing the population and identification of bad actors in the country, that commanders must be creative and persistent in their efforts to enroll as many Afghans as possible.

Chapter 2

Afghan Theater Overview: Impact on Biometrics

Introduction

Afghanistan is a very challenging environment to employ biometrics. Harsh terrain, limited infrastructure, and travel restrictions must be considered. Diverse languages, culture, and biometric equipment of coalition forces present significant operational challenges as well. This chapter examines environmental aspects of operations in Afghanistan and discusses their impact on biometrics employment. It also describes biometrics' principal organization, Task Force Biometrics, and discusses its organization and operational activities.

Operational Environment

Afghanistan lacks basic infrastructure such as paved roads and electricity. The lack of infrastructure is magnified by harsh terrain in much of the country. Steep mountains and isolated valleys naturally compartmentalize the country and have facilitated physical, cultural, and political diversification. Adjacent valleys have developed in dramatically different ways over the centuries, so there is no real "Afghan" national identity.

Over 40 nations comprise the International Security Assistance Force coalition. Several coalition partners operate closely with U.S. forces and Afghan National Security Forces (ANSF) collecting biometrics. Some countries deploy with biometrics equipment that may not be compatible with U.S. equipment, making the sharing of information extremely difficult. Commanders and leaders must be aware of differences in coalition biometrics equipment operating within their area of responsibility as well as usage limitations/restrictions to ensure gaps are covered. Lack of interoperability between coalition biometrics equipment sometimes requires downloading of biometrics data onto discs to transfer between systems.

Availability of a communications infrastructure and the ability to network collected biometric data in near real time can be a challenge, particularly among smaller bases. Moving biometrics personnel and equipment among these smaller bases can also be extremely complicated and time consuming due to the risks associated with ground/air movement and limited resources. This directly impacts security of U.S. forces when relying on coalition forces using their biometrics equipment for base access that cannot upload the theater-developed biometrics enabled watch list (BEWL). This may require employing different U.S. and coalition biometric equipment concurrently, resulting in dual enrollments of individuals. Such circumstances may require disconnected operations, hampering timeliness

of data exchange and may prevent some data sharing, such as intelligence-related information.

Biometric data movement within U.S.-operated networks can also be difficult due to data volume, file size, and network problems. One particular challenge is the movement of data from the Handheld Interagency Identity Detection Equipment (HIIDE) into the Biometrics Automated Toolset (BAT) network (Figure 2-1). The HIIDE is not capable of wireless data transmission; it must be physically attached to a BAT system for downloading biometric enrollments. Subsequently, the BEWL is uploaded to the HIIDE through the BAT. Tactics, techniques, and procedures are being developed to help overcome challenges of data movement. In some austere locations, the HIIDE may need to be transported to a BAT to download biometric data or upload the BEWL.



Figure 2-1. BAT kit

Figure 2-2 depicts the challenges of data latency, or the delay between enrollment and ingestion into the system. The greatest challenge to data latency is the enrolling unit's timeliness of uploading data. Units will report actual numbers of biometric enrollments, but will often wait several days (sometimes weeks) to upload the data. Enrollments can take up to five weeks to be ingested and replicated across the database, causing a delay in delivery of important information to other units. Ideally, units should download their enrollments within eight hours of completion of an operation to ensure appropriate action is taken for watch list individuals.

Troubleshooting and maintenance of biometric systems are completely dependent upon contractor support — field service engineers (FSEs). FSEs are located at various forward operating bases across the theater, but must often travel to smaller, more isolated facilities to provide service. Some requests for repair or replacement of biometric systems may be delayed due to the limited number of FSEs in theater.

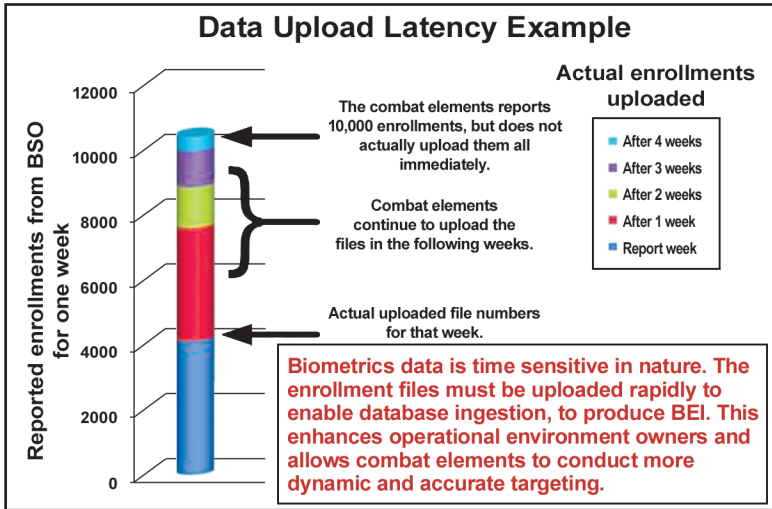


Figure 2-2. Data upload latency

The cumulative effect of these challenges constrains the coalition forces' ability to collect biometrics on Afghan citizens. To help overcome these challenges, coalition forces need to partner with the Government of the Islamic Republic of Afghanistan and eventually turn over biometric operations to ANSF. Operating with or in support of local and national security forces or tribal leadership can serve to expand the opportunities for biometric collections. When in doubt, consult your biometrics staff representative or Task Force Biometrics.

Chapter 3

Leader Responsibilities

Introduction

Leaders must ensure biometrics and its capabilities are leveraged to accomplish the assigned missions while protecting their personnel. This chapter discusses critical actions commanders and staffs must take to ensure effective integration of biometrics into the spectrum of operational missions. Some of these tasks are common to the employment of any combat-enabling capability, but some are unique, such as the need to plan for the upload of the current biometrics enabled watch list (BEWL) prior to conducting any operation.

Commander's Responsibilities

The commander sets the tone for biometrics in the unit. It is his responsibility to ensure biometrics are leveraged to the fullest extent possible to defeat the enemy, advance the interests of Afghanistan, and enhance Soldiers' protection. The commander can accomplish this in several ways:

- Demonstrating a belief in biometrics. Ensure the support staff and leaders do not treat biometrics operations as a check-the-block activity.
- Designate a biometrics subject-matter expert (SME). Ensure the SME is incorporated in all staff activities. This is critical for unit success. The SME will serve as the resident expert and primary liaison to Task Force (TF) Biometrics.
- Ensure personnel initially designated to perform biometric collections *stay* assigned to perform biometric collections. Failure to dedicate good Soldiers to this mission ensures training received will evaporate quickly.
- Stress proper collection techniques. Improper or partial biometric collections wastes time and leads to gaps in knowledge of the enemy. This creates seams for insurgents to exploit and could allow a very important insurgent to slip through. Quality biometric collections will lead to a greater degree of force protection for the unit and local population.
- Ensure the operations staff officer (S-3/G-3) coordinates and incorporates new equipment training (NET) and doctrine and tactics training (DTT) in the predeployment work up. Fully leverage opportunities at the combat training centers (CTCs) to hone biometrics skill sets.

- Ensure staff elements incorporate biometrics planning into every operation. Ensure biometrics collection capabilities are available for all site exploitation events. The more enrollments conducted, the larger the database. The larger the database, the more likelihood of success in finding those responsible for targeting and killing our service members.
- Leverage capabilities of the company intelligence support team (COIST) into all operations. This is a powerful tool for the commander and his staff and must be used to the fullest extent possible. Fuse biometrics with all the other intelligence you receive.
- Demonstrate an understanding of the value of biometrics — staff and subordinates will notice. Use biometrics background data in negotiations with local elders or *maliks*. It gives an extra edge in verifying when they are telling the truth or when they are trying to misdirect you. In this way, biometrics allows commanders to “protect the people from malign actors as well as from terrorists” (International Security Assistance Force [ISAF] *Commander’s Counterinsurgency [COIN] Guidance*, 1 August 2010).
- Work closely with local leaders in the unit’s area of operation (AO); gain their acceptance and support of biometrics enrollment activities.
- Stress biometrics collection and exploitation in the commander’s guidance. Ensure biometrics is included in every operations order (OPORD) and fragmentation order (FRAGO) issued by your headquarters. This will increase the number of quality enrollments in the AO. While numerical enrollment requirements can help emphasize the importance of collections, it may also push Soldiers to take shortcuts and compromise the quality of enrollments.
- Make biometrics preparedness a part of the unit’s pre-execution checklist. Checks should ensure all handheld devices have the most up-to-date watch lists available.
- Post-mission actions must include downloading and transmitting all new biometric enrollment data in the quickest way possible. In some cases, this may require physically moving the data or collection system to a location where it can be transmitted into the theater biometrics network.

Biometrics operations are currently hampered by a lack of doctrine, organization, standardized training, and shortage of equipment available for home station training and a lack of dedicated, assigned personnel. However, commanders can make the difference simply through leadership. Demand that biometric requirements be met. Leadership can make the difference in all these shortcomings.

Mission Planning

Biometrics is an extremely powerful nonlethal weapon for the COIN fight. Biometrics gives us the means to separate combatants from the populace very effectively in an unobtrusive way. To achieve biometrics' maximum effect, Soldiers must train on it, plan for its employment, and carefully rehearse its role in operations. Planning for the enrollment mission should account for all events — from departure of friendly lines or insertion to re-entry of friendly lines or extraction. Mission planners should have Afghan National Security Forces (ANSF) leading biometrics operations whenever possible. Unit standing operating procedures (SOPs) and mission checklists are valuable in helping planners concentrate on the unique aspects of the operation. Biometric support elements are available at the regional command level to provide planning and analytical expertise and products for the unique employment of biometrics to support a variety of missions.

Achieving the full effects of biometrics on the battlefield requires its inclusion in planning from mission receipt to the after-action report. Some of those effects are:

- Stripping the insurgent of his anonymity.
- Separating the insurgent from the populace.
- Promoting security and governance.
- Increasing confidence in our coalition partners.
- Creating complex terrain and denying the enemy freedom of movement.
- Mapping the “human terrain.”
- Enhancing force protection and control access to facilities.
- Identifying, tracking, and exploiting persons of interest (POIs).
- Supporting the targeting and identifying of networks in the counter improvised explosive device (IED) fight.

To fully leverage biometrics, commanders and their staffs must incorporate it throughout the military decisionmaking process:

Receipt of mission

- At the very inception of the planning process, the commander and the S-3 should be thinking of ways to leverage biometrics in their operation.

Mission analysis

- If not specified, biometrics collection must be considered an implied mission in a COIN environment.
- When analyzing task organization, consider adequate availability of biometrics collection equipment and arrangement for augmentation if necessary.
- Infuse biometrics collection capabilities during the intelligence preparation of the battlefield (IPB) and document outcome (e.g., canalizing traffic to checkpoints and identifying key houses/businesses).
- Commander's guidance must address employment of biometrics collection systems in:
 - Commander's critical information requirements.
 - Reconnaissance guidance.
 - Deception guidance.
 - Fire support guidance.
 - Mobility and countermobility guidance.
 - Security measures.
 - Time plan.
 - Types of rehearsals to conduct.

Course of action (COA) development

- Biometrics should be included at the appropriate level in each COA. The array of initial forces should incorporate biometrics collection elements. Plan to put ANSF in the lead whenever possible.
- Biometrics should be fully embedded into the targeting process.

COA analysis

- When conducting COA analysis, careful consideration should be given to potential enemy reactions to friendly biometrics collections.
- Refine the incorporation of biometrics collection in the synchronization matrix.
- Refine task organization as required to accomplish the biometrics collection mission.

COA approval

- Biometrics collection must be incorporated in specified rehearsals.
- Biometrics collection and the use of BEWLs should be included in the high-pay off target list, as appropriate.

Orders production

- Biometrics collection and/or exploitation should be included in every OPOD to the extent appropriate for the operation.
- Biometrics must be included in the reconnaissance and surveillance plan as well as the collection management plan.
- Biometrics is a key part of the common operational picture.
- Biometrics may also lead to its own branches and/or sequels.
- Synchronization of all aspects of the operation should incorporate biometrics functions.
- Biometrics must be included in the information network.
- Biometrics must also be considered an operational security measure.

Staff Elements Responsibilities

Every staff element has a role in ensuring the proper incorporation of biometrics into mission accomplishment. By the same token, every staff element can utilize the biometrics collections system in some capacity. Planning operations to incorporate biometrics systems takes minor coordination.

Intelligence staff officer

Biometrics serves the intelligence staff officer (S-2) several ways in day-to-day operations. Below are recommended tasks that provide the S-2 with a complete picture when conducting IPB or identifying key elements of local networks.

- Biometrics-enabled intelligence (BEI) personnel at theater and above can create products that fuse biometrics information with terrain analysis (in effect, biometrics-enabled IPB). These products can be invaluable in planning operations that can lead to improved biometrics collections. For example, some products will actually become recommended named areas of interest (NAIs) for the collection of biometrics and are likely to result in matches against the theater BEWL or against unknown latent files. Much of this type of analysis — termed human terrain mapping — is currently produced by the National Ground Intelligence Center (NGIC) in conjunction

with TF Biometrics BEI personnel. The S-2 can also create a density study that is simply a geospatial product that depicts “hot spots” of a given activity — it is not specific to biometrics. This can be watch list encounters, biometric enrollments, IED events, etc. Figure 3-1 demonstrates how BEI can create products showing “hot spots” of “latents of value” within an AO that can then be used to nominate NAIs and show trends driving future operations.

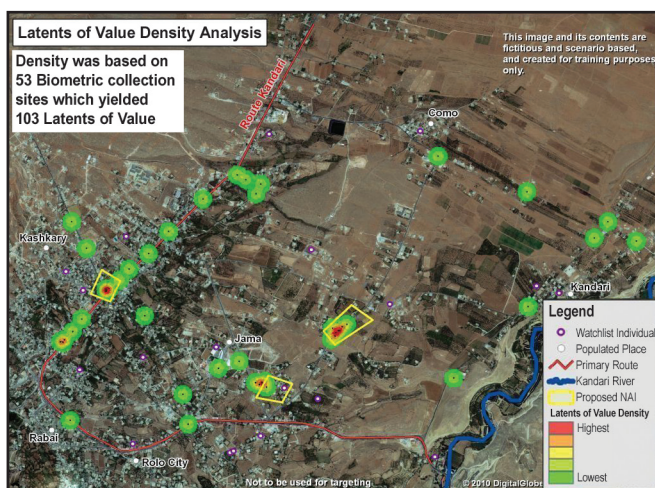


Figure 3-1. Latents of value density analysis

- Data from the biometrics automated toolset (BAT) system can be incorporated into the Tactical Ground Reporting (TIGR) System network to plot locations of watch list hits or enrollments using the BAT capture location field. The Distributed Common Ground Station–Army (DCGS–A) can now index on 13 tables from the BAT record. All attachments associated with the record are included and listed by filename, and associated persons identified are actively linked. This is done through a BAT feed into the Query Tree database with a live feed into the ArcMap mapping tool.
- BEWL hits should be immediately reported through the chain of command and to theater biometrics intelligence personnel. All appropriate actions should be taken in response to the hit. Knowing the nomination process for a local alert or nomination to the NGIC level will help keep a POI off another forward operating base (FOB) or combat outpost when the individual has been caught in suspicious activities. For example, a local national caught on a FOB for stealing, fighting, or mapping the location can be nominated to the BEWL if

you want the individual kept off other locations. A tracking report should be completed on all watch list hits.

- Targeting is enhanced through the use of biometrics by positive identification of the target. The photo can assist when conducting a cordon and search or other type of search activity. Fingerprints and iris collection for identification or verification on site can help confirm individual target identification. Individuals targeted for operations are usually on the theater BEWL, but their associates may not be. Requesting biometrics on these non-watch listed personnel may be valuable in locating the primary target.
- Mapping the human terrain can contribute markedly to overall area security. Knowing who belongs in a village — who they are, what they do, to whom they are related, and where they live — all helps to separate the locals from the insurgents.
- Whenever possible, commanders and staff members should provide feedback to the biometric collectors when the organization has a successful biometrics “hit” or succeeds in either taking an insurgent out of the fight or laying the groundwork for someone else to take him out of the fight.

Operations staff officer

Biometrics collection and utilization is primarily an operations function. Like any other weapon system, lethal and nonlethal, it must be incorporated into the unit’s synchronization matrix and provision made for its full employment. By using biometrics properly, the S-3 separates the insurgent from the populace, rendering him vulnerable to coalition activity (Figure 3-2). As noted in *ISAF Commander’s Counterinsurgency Guidance*, our operations are most effective “when the insurgents have become so isolated from the population that they are no longer welcome, have been kicked out of their communities, and are reduced to hiding in remote areas and raiding from there.” Biometrics allows an almost foolproof means of identification that is noninvasive yet extraordinarily accurate. Using biometrics collections along with other forensics capabilities will ultimately secure the area for both coalition forces and the local populace.



Figure 3-2. Example of an insurgent match

- There are many areas an S-3 can incorporate biometrics-related information and collection devices during staff activities: mission assessments, developing COAs, conducting IPB, and in developing OPORDs, warning orders, and battle update briefs.
- Integrate biometrics into unit tactical SOPs to include processes for downloading updated BEWLs, reporting hits against the BEWL, and downloading/transmitting biometrics enrollment data at the end of a mission. This should be a key part of a unit's battle rhythm.
- Collection and use of biometrics should become part of a unit's priority intelligence requirement that seeks information on the local population or a specific information requirement that directs collection in a set location. If an increase of IEDs has occurred, consider FRAGOs that set up traffic control points to screen against the watch list and create NAIs for future cordon and search operations. Additionally, biometrics is a dramatic enabler for conducting census operations and allowing the unit to positively link individuals with activities and locations.
- Facts can be provided on the total number of collections conducted in an area. Assumptions can include that an increase in collections will result in an increase in identification of those on the watch list and will result in a reduction of hostile activities against friendly forces and increased force protection.
- A new equipment training/doctrine training team (NET/DTT) training event should be planned at home station prior to conducting a mission rehearsal exercise (MRE). The NET/DTT will provide training for COIST Soldiers and intelligence analysts in the S-2 and S-3 sections. Once the training is completed, the unit can request home station training equipment from the program manager — Department of Defense Biometrics Identity Management Agency and trainers can assist during any lane training or other training exercises in preparation for the MRE. Biometrics can also be incorporated into all training at the CTCs.
- Biometrics can and should be incorporated into every operation conducted by the unit. Chapter 4 of this handbook discusses biometrics contributions/considerations for most types of missions a unit will conduct in Afghanistan.
- Biometric collections are most often planned in conjunction with other missions; collections may also be the focus of the mission, particularly when building up the knowledge of the local populace (a.k.a. mapping the human terrain).

Logistics staff officer

The logistics staff officer (S-4) plays a critical role in ensuring equipment can be replaced and is available for operations. Placing information in the staff estimate on the availability of the equipment and the time it takes to replace non-operational items can assist units planning for operations. This helps when equipment may need to be cross-leveled for one unit that will be fully engaged in conducting operations while another may not. Coordinating with and informing the command, control, communications, and computer staff officer (S-6) of newly received equipment will help with the primary, alternate, contingency, and emergency (PACE) communications plan. Making contact prior to deployment with the field service engineers (FSEs) and the manager of theater-provided equipment for biometrics equipment will ensure a smooth transition and increase the availability of equipment.

Command, control, communications, and computer staff officer

The S-6 must incorporate biometrics collections systems into the PACE communications plan. A communications architecture plan should be developed that supports the PACE plan and that can be used to brief system status. BAT will need dedicated Internet protocol addresses on the SECRET Internet Protocol Router Network, and there are bandwidth constraints that can be identified prior to deployment. Units may still receive updates through the use of portable hard drives and digital video disks. The BAT FSE can assist in troubleshooting and repairing equipment when there are problems.

Company intelligence support team

The COIST has the BAT, Handheld Interagency Identity Detection Equipment (HIIDE), and the DCGS-A basic analyst laptop (BAL) available for its use to diminish the adversary's capability to hide among the populace. The TIGR network is used in Afghanistan to pull in BAT data and use it to track POIs. The biometric and biographical information collected by the Soldiers with the BAT and HIIDE will be used to build linkages between inhabitants within the AO. The BAL, with the ingestion of BAT data, can plot and compare other operational events, such as sniper or IED attacks, to give a better picture of local networks and locations.

As an example, a biometric enrollment matches a local electronics shop dealer to the BEWL and leads a team to question the dealer regarding the increase in remote-controlled IED events in the local vicinity. Due to an increase in IED activity, the COIST may suggest to the commander to complete a biometric survey of the local bazaar. After completion of the survey, Soldiers will issue badges to all the vendors. An approved vendor

list is loaded on the HIIDE device, and Soldiers will complete periodic biometric sweeps looking for unauthorized vendors or watch listed individuals. As Soldiers move through the bazaar, signals intelligence assets may see an increase in cellular phone traffic. These actions might not only lead Soldiers to an unauthorized person, but also identify people in the local insurgency network.

By fully incorporating biometrics in the planning process and leveraging the full array of capabilities it bestows on units, we can make a difference in both our AO and in the long-term fight. “We (ISAF and Government of the Islamic Republic of Afghanistan) will succeed by transforming the environment through local security, connecting responsive and credible governance to the community leaders and the people, and facilitating compelling alternatives to the insurgency.” (ISAF *Commander’s Counterinsurgency Guidance*)

Chapter 4

Biometrics Support to Operations

Introduction

Biometrics can support virtually every operation conducted in Afghanistan. Offensive, defensive, stability, and support operations are all enhanced by incorporating biometrics. Biometrics can play a key role in any operation where you need to know exactly with whom you are dealing — friend, foe, or unknown. In addition, most operations can provide an opportunity for the collection of biometrics, which in turn builds up the database and makes identification of insurgents more likely in the future. Of course, these operations must be planned and rehearsed to be effective. In support of all operations, the frequent uploading of a current watch list on all handheld devices like the Handheld Interagency Identity Detection Equipment (HIIDE) and stationary devices like the Biometrics Automated Toolset (BAT) is absolutely critical and should be made a standard part of the unit's battle rhythm.

All biometric usage in Afghanistan must conform to International Security Assistance Forces (ISAF) and the Government of the Islamic Republic of Afghanistan rules governing the collection of biometrics. Units will face some constraints they may not have experienced in Iraq; this may include a general aversion to mass involuntary enrollments that were conducted in Iraq. However, as a general rule of thumb, operating with the concurrence of local tribal and governmental leadership — and with the assistance of the Afghan National Security Forces (ANSF) — a unit can dramatically expand the opportunities for using biometrics.

This chapter will address some of the specific roles biometrics can play in different types of operations.

Offensive Operations

Cordon operations

To find selected personnel or material, a unit will typically conduct a cordon and search or cordon and knock operation. There are two primary elements in a cordon and search operation — the cordon element and the search element. Both of those elements have requirements for biometrics capability. 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, biometrics can be used effectively. The cordon element can also set up checkpoints with biometrics systems that can be used to screen individuals seeking to enter or leave the

cordon area. Some of the considerations for biometrics employment in a cordon operation include:

- Plan for biometrics in the operation order/fragmentary order.
- Plan biometrics enrollments and screening.
- Ensure watch lists and local alerts are loaded before the mission.
- Use biometrics checkpoints in the cordon to canalize traffic.
- Positive/negative identification of target(s).
- Ensure company intelligence support team data downloads are incorporated into debriefs.
- Enroll everyone, to include all enemy casualties (wounded and killed).

Targeted operations

In Joint Publication 3-0, *Joint Operations*, targeting is defined as “the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.” Targeting is essentially the identification of personnel or objects that must be killed, captured, or destroyed. To undertake targeting operations, one must be aware of how biometrics/exploitation and the other multidisciplinary intelligence and operational enablers can assist the commander to synchronize intelligence, maneuver, fire support systems, nonlethal systems, and special operations forces by attacking the right target, with the best system, at the right time. Accurate identity and attribution is crucial when targeting individuals hidden among the population.

To achieve a targeting effect in the operational environment, a targeting process must be followed that provides an agile force with enough accurate and timely information to allow them to interdict, kill, capture, recover, observe, engage, or substitute personnel, materiel, or information. The doctrinal army targeting process is the decide, detect, deliver and assess (D3A) process as stated in Army Field Manual (FM) 3-60.1, *Multi-Service TTP for Targeting Time Sensitive Targets*. Biometrics certainly supports this process as part of a multidisciplinary effort; however, the emerging find, fix, finish, exploit, and analyze (F3EAD) targeting methodology (Figure 4-1) perhaps better allows for identity-focused targeting and the full capability of technical exploitation to be realized and applied. It is not a substitute for D3A, but is a subset designed for a specific targeting requirement that refines the actions to be complete when engaging high-value individuals (HVIs).

Figure 4-1 pictorially depicts the linkages between D3A and F3EAD, and how biometrics and exploitation enhances the overall targeting process.

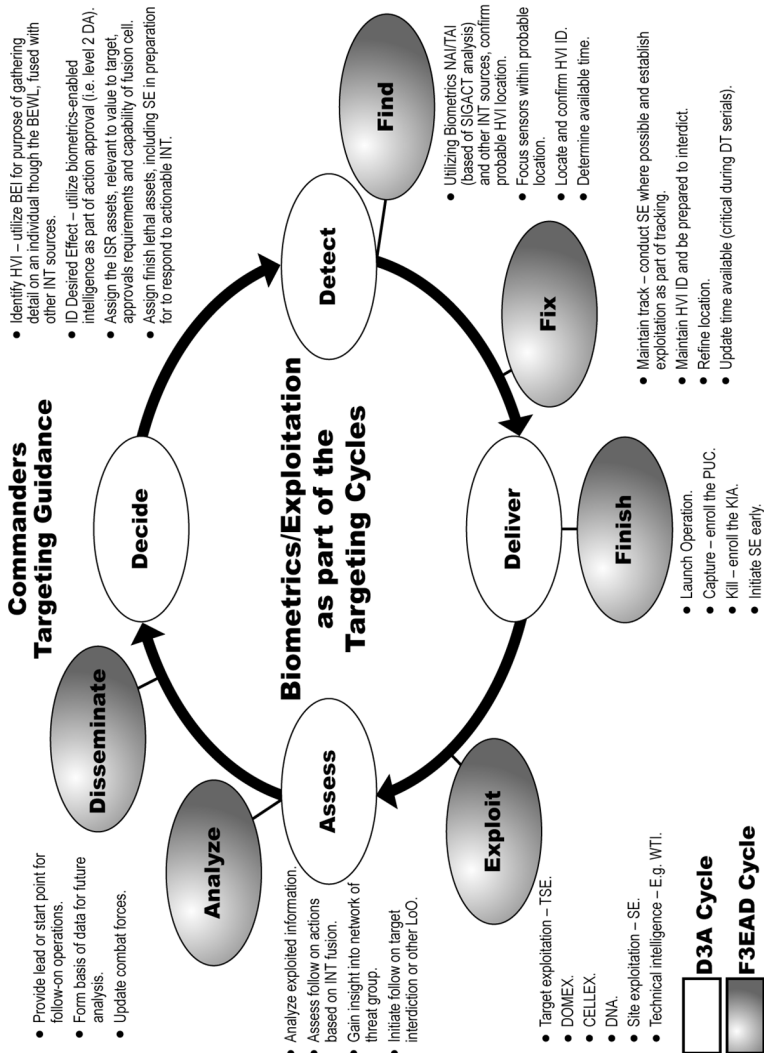


Figure 4-1. Biometrics in targeting process

(The steps of the targeting process are further broken down in FM 3-60.1.) For purposes of dynamic targeting, another subset of D3A is the find, fix, track, target, engage and assess process. Although the inputs of biometrics/exploitation are easy to demonstrate for this process, it will not be discussed further in this document.

Population management

Identifying the population in a particular area is essential to effective counterinsurgency operations (Figures 4-2 and 4-3). A unit “owning ground” in a combat zone needs to know who lives where, who does what, who belongs, and who does not. In Afghanistan, population management (or census) efforts are often seen as supportive of the local government, particularly if accompanied with a badging program that highlights the government’s presence in an area. Tribal leaders and clan heads can use biometrics to secure their populace against outsiders who arrive for the purpose of intimidation or other negative activities. Simply knowing who belongs in a village automatically spotlights those who do not. These operations can also lend authority to tribal leadership by helping them keep unwanted individuals out of their areas.



Figure 4-2. Population management



Figure 4-3. Roadside enrollment

Every person who lives within an operational area should be identified and fully biometrically enrolled with facial photos, iris scans, and all ten fingerprints (if present). This information should be coupled with good contextual data, such as where they live, what they do, and to which tribe or clan they belong. In this manner, a unit can easily identify outsiders or newcomers. This information is also useful in the transfer of authority to another unit; a unit inheriting an effective census can become much more effective in a much shorter time frame. Population management actions can also have the effect of building good relationships and rapport. The message can be crafted that the census is intended to protect them from the influence of outsiders and will give them a chance to more easily identify troublemakers in their midst. Population management operations offer excellent opportunities to:

- Locate and identify every resident (visit and record every house and business). At a minimum, fully biometrically enroll all military-age males as follows:
 - Full sets of fingerprints.
 - Full face photo.
 - Iris scans.
 - Names and all variants of names.
 - BAT associative elements:
 - * Address.
 - * Occupation.
 - * Tribal name.
 - * Military grid reference of enrollment.
- Create an enrollment event for future data mining.
- Listen to and understand residents' problems.
- Put residents in a common database.
- Collect and assess civil-military operations data.
- Identify local leaders and use them to identify the populace.
- Use badging to identify local leaders, and key personnel.
- Cultivate human intelligence sources.

- Push indigenous forces into the lead at every possible opportunity.
- Track persons of interest; unusual travel patterns may indicate unusual activities.

Detainee operations

Personnel detained for any reason should be completely biometrically enrolled as quickly as possible following initial detention. Personnel detained for one reason may be found to have several reasons for a unit to detain them. The additional information available in the biometric database may be sufficient to support the decision to continue to detain the individual past the 96 hour ISAF window. At a minimum, it provides a tracking tool for every individual detained for whatever reason across the country. It also provides a highly effective interrogation tool in that the interrogator knows for sure that a detainee was in “Khost a week ago” and in “Helmand a month ago.” Such specific information is of great use in interrogation. Biometrics can also help to identify detainees who are not on the biometrics enabled watch list (BEWL) and should be. When integrated into the overall detainee tracking/management process, biometrics can help verify and support the decision to release or transfer an individual. Biometrics allows a unit to:

- Positively identify detainees with biometrics.
- Track details of interactions with detainees throughout the detention process, to include release.
- Prepare for effective interrogation by checking the BEWL and other activities.
- Attain convictions through latent matches.

Checkpoint operations

Checkpoints have a variety of functions — from controlling access to specific areas, to canalizing traffic, to positively identifying those who are passing through a given area. Checkpoints are frequently used to support other operations. Biometrics can support checkpoint operations in a number of ways, not the least of which is to positively identify those passing through the checkpoint. To be most effective, units should:

- Canalize all traffic to checkpoints.
- Use “overwatch” to spot individuals trying to avoid checkpoints.
- When practical, badge all residents, or males, or military-aged males.

Toxic industrial chemicals or improvised explosive device events

Units that engage the enemy or who are involved in an improvised explosive device event should enroll all nearby individuals after they have secured the area. Triggermen or spotters may be in the crowd or in “overwatch” positions. All enemy casualties should also be enrolled, even if you come upon them hours or more after an event. This information can prove invaluable to the intelligence effort.

Defensive Operations

Personnel screening

U.S. forces use a number of locally hired personnel in deployed areas for a variety of reasons. Local hires are essential to the effective operation of forward operating bases and can be found on virtually every installation operated by U.S. forces. Biometrics should also be used to screen those who will receive Commander’s Emergency Response Program funds for locally managed engineering projects. This will help prevent U.S. taxpayer dollars going to support the insurgency. Most importantly, all ANSF or local security forces that receive training by U.S. or ISAF must be screened to ensure they are not members or supporters of the insurgency. Units are highly encouraged to:

- Enroll all locally employed personnel and third-country nationals working on the base.
- Enroll all non-U.S. contractors working on the base.
- Enroll all local contract awardees.
- Enroll all local personnel receiving military training.
- Require biometrics “signatures” to receive payment.

Base access/force protection

Biometrics is a powerful force protection tool, and U.S. units are required to employ biometrics at the entry control points (ECPs) for most U.S.-controlled facilities. However, some units are not fully using the capabilities available or are not using them correctly, allowing dangerous gaps to develop that can be exploited by the enemy. In 2004, an Iraqi national used his brother’s non-biometric base access card to conduct a devastating suicide attack on a mess hall in Mosul. Biometrically enabled access cards, used in conjunction with a regular screening process at the ECP, can prevent such attacks by positively identifying the bearer of the access card.

- Fully enroll all personnel who will be allowed regular access to your installation and issue them a biometrically enabled access card. Regardless of past efforts, do not assume this has been done.
- Biometrically screen all personnel entering or leaving the base, even if they possess an access card. A handheld system using an iris scanner can do this very quickly.

Border control and port of entry management

Biometrics is extremely effective for managing and tracking cross-border movements. Our enemies may find sanctuary across a border, but biometrics can make the task of returning an extraordinarily risky venture. Biometrics immediately creates complex terrain for the enemy by limiting the corridors they can use to return to Afghanistan. Tracking personnel at ports of entry and border crossings produces a great wealth of information on their movements. Repeated crossings show a pattern of behavior that can reveal a number of things, from migration patterns to supply routes. Simply identifying the routes of merchants can identify a significant pattern. In Afghanistan, formally recognized border crossings will operate under the control of the Afghan Border Police, who will help direct personnel to enrollment stations. To be most effective, a unit should:

- Canalize all traffic to ports of entry and border crossing enrollment locations.
- Enroll as many personnel crossing the border as possible, traveling in both directions.
- Maintain “overwatch” on access routes to identify personnel attempting to avoid border control points.

Other Operations

Security assistance

Biometrics allow a commander to empower his counterparts in the national security forces by providing positive identification of their forces. This ensures a commander’s forces have not been infiltrated by the enemy and adds to the legitimacy of his forces by increasing confidence among the populace that they are truly national forces and not personnel masquerading as such. Whenever possible, a unit should:

- Enroll/screen all local police, army, and security forces.
- Use biometrics as a means to work more closely with host-nation forces (help your counterparts to be a success by culling undesirables from their ranks).

- Inform commanders about the true background of some of their personnel (an Afghan policeman might prove less effective as a policeman if he has previously been banned from an American base for stealing).

Recovery operations

Recovery operations may be intentional or unintentional. A unit may be actively seeking a Soldier, Airman, Sailor, or Marine held prisoner or a hostage in the area, or may simply find one in the course of a cordon and search operation. A unit might also be approached by a person claiming to be someone in particular. Biometrics supports commanders in recovery operations by:

- Ensuring the individual you are seeking is the one you have in your hands.
- Positively identifying a body, regardless of the integrity of a corpse.
- Ensuring the person you have encountered is, in fact, who he claims to be.

Humanitarian assistance

Humanitarian assistance can be provided for a number of reasons, both natural and man-made. The distribution of aid, however, should be carefully controlled to ensure everyone gets their “fair share” without anyone being able to stockpile or hoard relief supplies. This ensures there will be sufficient supplies of aid and that no one truly benefits from a disaster (and, of course ensures we do not inadvertently deliver aid to our enemies). It should also prevent availability of relief supplies on the black market, which is harmful to both U.S. and Afghanistan interests. To be most effective, use biometrics to:

- Enroll all recipients of humanitarian assistance to ensure no “double dipping” into humanitarian assistance resources.
- Reunite families after a disaster (using DNA).
- Ensure we do not provide aid to anyone on the BEWL or who has had a latent print recovered from a site of anti-coalition activities.

Medical/dental

In the same manner that humanitarian assistance may be controlled by the use of biometrics to prevent profiteering, so medical assistance lends itself to the same function. However, with medical assistance, it can have an even more positive impact by ensuring someone does not receive the same inoculation twice or gets more medicine than they really need. Many

people in rural areas do not understand why the medicine they receive works so well and often have the philosophy, “If some is good, more is better.” Biometrics can allow positive control of the distribution of medical assistance and ensure that no one receives more than they should. Use biometrics to:

- Enroll all recipients of medical assistance to ensure no “double dipping” into medical resources.
- Determine impact of care given and validate no “free” medical care is given to those on the watch list.

Chapter 5

Biometrics-Enabled Intelligence

Introduction

Fusion of disparate information or intelligence related to a person or biometric identity to other people (identities), events, activities, combined with economic, population, and governmental atmospherics provide a higher level of fusion/analysis to attack the insurgent network or “find, fix and finish off enemy leaders.”¹ The intent of biometrics-enabled intelligence (BEI) is to identify an individual and link that individual to broader groups through all-source intelligence capabilities, including biometrics, forensics, document exploitation, cell phone exploitation, and media exploitation.

Biometrics-Enabled Intelligence in Afghanistan

Biometrics in Afghanistan centers on denying the enemy anonymity among the populace. Biometrics are unique and can positively identify an individual. Linking intelligence products, operational information, or other data to a biometric record and placing an individual on the biometrics-enabled watch list (BEWL) is the simplest form of BEI.

In Afghanistan, BEI analysts are being deployed to the brigade combat teams, special operations elements, regional commands (RCs) (division level), and other coalition forces/elements by request. The duties of the BEI analyst are very broad in spectrum and continue to develop. To be successful, BEI analysts must integrate with the intelligence staff officer and operations staff officer to provide subject-matter expertise on the meaning of biometric and forensic matches when combined with traditional intelligence, contextual, and combat information. The BEI analyst also coordinates for the development of BEI products in support of force protection, operational planning, and intelligence activities. The BEI multiechelon structure allows for development of more complex and comprehensive products.

There are several BEI organizations providing support to the forward deployed BEI analyst: the theater BEI cell at Bagram Air Base; 513th Military Intelligence (MI) Brigade at Fort Gordon, GA; and the Biometrics Intelligence Program (BIP) at the National Ground Intelligence Center (NGIC) at Charlottesville, VA. Requests for development of BEI products are processed 24 hours a day, 7 days a week by imbedded BEI analysts or the theater BEI cell and are elevated to the proper organization based on suspense time, complexity, and available resources.

Biometrics-Enabled Intelligence Analyst

BEI analysts are the supported unit's subject matter experts providing intelligence relevance for biometric collections, biometric and forensic matches, and watch list hits. They also provide all-source intelligence analytic support and coordination for complex BEI products in direct support, when assigned to a specific unit, or in general support roles at the RC or theater level. The following are specific examples of the support BEI analysts provide:

- **Watch listing.** One of the primary duties of the BEI analyst is to manage watch list processes for the unit's collected biometric identities and link related contextual information and intelligence to properly document the records for future reference or further analysis.
- **Answer immediate requests for information.** The BEI analyst is the point of contact for providing immediate feedback to entry control points, counterintelligence screeners, or tactical elements on the watch list status and providing a quick summary of information on subjects encountered.
- **Enhancement.** Enhancement is the process of linking related intelligence or operational reports to a biometric record or identity. Historically, biometrics collected during planned operations or during meeting engagements have incomplete contextual information on where, when, or why the person's biometrics was collected. Patrol reports are invaluable to providing answers to why subjects are enrolled. The analysts must coordinate with the unit's collectors to link the missing contextual data to the biometrics or research the data from sources such as the Tactical Ground Reporting (TIGR) System, the Combined Information Data Network Exchange, Command Post of the future, significant activities repositories, Combating Terrorism Center Harmony database, Distributed Common Ground Station–Army (DCGS-A), and unit journals.
- **Coordination for analytic products.** The BEI analyst supports a unit's mission planning through the coordination for BEI products. When specific biometric analytic products are required, the analyst gathers all related information and forwards the data to the respective BEI organization for development.

Biometrics-Enabled Intelligence Products

The following are the current BEI products that analysts can develop through their reach-back capabilities to the theater BEI cell, NGIC, or the 513th MI Brigade:

- **Biometric identity analysis report (BIAR).** The BIAR is a “processed” intelligence product that associates a biometric match with an individual in the biometrics database. The BIAR is produced by sorting, analyzing, and linking the biometric match with the individual’s history — along with all sources of intelligence. It contains the identification, background, and assessment of the threat as well the intelligence value of the subject. The report is produced for all latent matches, other high-threat matches, and matches from specified mission areas. Customers may request BIARs directly from the NGIC through the deployed BEI analyst for other matches.
- **Biometric named area of interest (NAI).** This product is developed through forensically exploited information, geographically and/or biometrically related intelligence reporting, watch listing, and the standard intelligence preparation of the battlefield/NAI process. This product is designed to inform customers of the most operationally pertinent locations to conduct biometric collections to effectively capture targets of significance.
- **Biometric-focused area study (BFAS).** The BFAS is produced for customers who provide the BEI analyst with a predetermined location. The resulting BFAS provides customers with all of the forensically exploited biometrics, biometric NAIs, biometric collections, BIARs, and watch listed personnel from that predetermined location.
- **Biometric analysis packet (BAP).** The BAP provides identities of personnel who are biometrically enrolled or watch listed for a specified location. In addition to providing the identity of the individual, the BAP provides a brief background summary of the personalities associated with the individual.
- **Analytic case study/report.** A case study or assessment is conducted in support of large forensic and biometric cases where multiple subjects are involved. The studies include but are not limited to link analysis, threat assessments on known or unknown individuals, possible leads or source-directed requirements for counterintelligence, military police, law enforcement intelligence, or human intelligence. Studies can also be conducted to reveal trends or patterns of biometric and forensic matches.

- **BEWL.** A watch list is used to identify persons of interest (POIs). The Department of Defense (DOD) BEWL identifies POIs by biometric sample, not by a name or alias. In Afghanistan, the BEWL is divided into five Task Force (TF) Biometrics specific levels. Upon encounter and subsequent biometric enrollment, an alert will appear in certain biometric collection devices (e.g., Biometrics Automated Toolset [BAT], Handheld Interagency Identity Detection Equipment [HIIDE], and Secure Electronic Enrollment Kit [SEEK]). A tracking report should be completed on all individuals who are encountered on the watch list.

Watch Listing Explained

The linking of information or intelligence products to a biometric record and placing an individual on the watch list are the simplest forms of BEI. Listed below are the different levels associated with watch listing:

- Level 1 (detain) — A high threat individual with an International Security Assistance Force (ISAF)-approved target packet.
- Level 2 (question) — An individual with possible information of value who needs further questioning or a high-threat individual pending an ISAF-approved target packet.
- Level 3 (assess) — Allows for a tracking report for records of biometric enrollment of POIs for DOD to gather additional information. (Note that this field is not utilized in the Operation Enduring Freedom [OEF] theater).
- Level 4 (disqualify) — An individual who is denied base access, training, or employment due to his previous or potential threat to coalition forces.
- Level 5 (deny) — Criminal-based level. A denial of base access for an individual who has violated base policy but is not deemed a serious threat to coalition forces.
- Level 6 (track) — Not an actionable level. Report the location and purpose of movements of an individual to determine the individual's activities and associations.

Biometrics Enabled Watch List Nomination Process

To nominate an individual to the BEWL, provide an existing biometric for the individual and an appropriate justification to the level of the nominated individual. Anyone associated with coalition forces can nominate an individual either through a TF Biometrics representative or through the nomination tool in the biometric intelligence resource (BIR) program.

Biometric Identification Analysis Report (BIAR)

- Associates a biometric match with an individual.
- Produced by sorting, analyzing, and linking the biometric match, the individual's history, and all sources of intelligence.
- Contains the biographical information, identities, background, and associates of the individual.
- Provides an evaluation of the individual's activities and associations and determines threat and intelligence assessments.

Biometrics-Enabled Intelligence Tools

In addition to the ability to collect biometrics and the contextual data related to the collection, BAT has a tremendous ability to relate and attach documents, analytic comments, location data, and numerous other items to a record for future reference.

To assist in the publication and retrieval of BEI information, NGIC developed two web-based tools. These tools allow customized searches for individual records, biometric matches, and finished intelligence reporting associated to a specific individual. Both toolsets are on the SECRET Internet Protocol Router Network and require a username and password.

Automated Identification Management Systems

This system has an integrated workflow, web publishing, and production management tool for BEI. It assists in managing large volumes of collected biometric data being analyzed by BEI analysts and is the primary BIAR tool for authoring and dissemination. It allows advanced searches across BEI products and Automated Biometric Identification System (ABIS) biometric match data. "Customers" access Automated Identification Management Systems (AIMS) functionality through web-based interfaces to search for finished intelligence and biometric data on persons and populations of interest. Intelink Passport accounts require AIMS read-only access.

Biometric Intelligence Resource

Biometric intelligence resource (BIR) is the central repository for the automated aggregation, analysis, and dissemination of biometric samples and associated contextual, situational, and analytical data. It has full access to BAT data; AIMS BIARs; ABIS; and sensors such as HIIDE, BAT, Crossmatch Jumpkit, and others. BIR graphically links biometric encounters into a fused identity. BIR is available on multiple networks, making the raw data and finished intelligence products available to many different user communities in support of DOD and national missions.

Lessons Learned from Afghanistan

One size BEWL does not fit all. NGIC drives the watch list process and standards. As the use of biometrics, legal aspects, and rules of engagement evolved, host-nation laws and other issues required changes in the language and procedures used in BEWL operations.

Biometrics Enabled Watch List — A “Living Concept”

Commanders, leaders, and analysts must understand and not be hesitant to adjust the BEWL level of an individual of interest. BEI will document each change for future reference and continue to monitor reporting and the subject’s activities to ensure the watch list level remains valid.

Biometrics-Enabled Intelligence Awareness and Education

As a result of the integration of biometrics and forensics with traditional intelligence disciplines, only a small community understands the “so what” behind biometrics collection and exploitation. Individuals at all echelons must understand the capabilities and limitations of the biometrics collection and exploitation process. Biometrics education will enhance the integration of biometric systems into tactical operations. Additionally, integration of biometrics collections into field exercises is an excellent way to train staffs, test operator abilities, and troubleshoot problems. Training can also incorporate other key players in biometrics operations, such as law enforcement, through the biometric exploitation process.

Currently in Afghanistan, feedback from biometric collections is not often provided to tactical elements on the ground. Service members take considerable time, under dangerous conditions, to collect biometrics, but rarely see any feedback from the exploitation and analysis of biometric collections. Efforts are underway to provide a feedback loop through the TIGR system, which is used for mission planning and reporting at the company level.

All biometric records with a grid coordinate are extracted from the biometrics system and ingested into the TIGR database. This database provides the unit a geospatially-represented feedback mechanism with different icons based on the watch list level assigned to an individual. This is currently a manual process conducted by database administrators, BEI analysts, and the TIGR team in theater. Automation of this process must be completed at the program manager level. Additionally, a partially automated solution has been worked in theater to push those records that are geospatially enabled to the DCGS-A system for exposure to the ArcMap mapping tool and Query Tree database.

Biometrics-Enabled Intelligence — The Way Ahead

The TF Biometrics intelligence section has created a protocol to facilitate biometric watch listing and analytic support to civil and law enforcement authorities. The cornerstone of any counterinsurgency effort is establishing security for the civil populace. The BEI analyst must work diligently with the appropriate foreign disclosure officer (FDO) to ensure classification of exploited materials and exploitation results are able to be provided to prosecutors and the host-nation courts.

BEI continues to evolve through the process of understanding biometrics, the conditions, and operations of the ever-changing battlefield. A profile and pattern of life can be created through linking data exploited from an individual's documents, phone, electronic media, and other biometric collections. The profile can then be used for lethal and nonlethal targeting proposes and allows intelligence channels further understanding of networks and insurgent operations.

Endnote

1. *Fixing Intel: A Blueprint for Making Intelligence Relevant In Afghanistan*, January 2010, MG Flynn, CPT Pottinger, Mr. Batchelor.

Appendix A

Basic Biometric Principles

What is Biometrics?

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, biometrics is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. A few of the current biological characteristics, commonly referred to as modalities, used to identify people are fingerprints, iris images, facial photos, certain types of voice patterns, palm prints, and DNA. Behavioral characteristics can be a signature, the keystroke pattern on a keyboard, certain types of voice patterns, and gait.

As a process, biometrics is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. For tactical biometrics, we use the terms interchangeably. Biometrics is used in two ways: verification and identification. Verification compares one biometric to an identified biometric (1:1) to verify that an individual is who he says he is. Identification compares one biometric to a database of biometrics (1:N) to find out who an individual is.

Tactical Collection Modalities

The most prevalent tactical biometric collection systems focus on collecting three specific modalities: fingerprints, iris images, and facial photos. These three modalities have proved to be the most tactically useful of all the modalities currently employed or under study. Fingerprints provide a means to identify where someone has been or what they have been doing, since they are often left behind on anything used or touched, to include exploded improvised explosive devices (IEDs). Iris images provide the most accurate (and fastest) means to positively identify a person once they have been enrolled in the system. Facial photos give a Soldier a visual means to identify a person and help complete a targeting package.

Why fingerprints, iris images and facial photos?

Within biometrics, there are seven widely accepted methods to measure the use and effectiveness of a modality. These seven measures are:

- Universality — The biometric is shared by all humans.
- Distinctiveness — The biometric is unique, constituting a distinguishing feature.

- Permanence — The biometric remains largely unchanged throughout a person's life.
- Collectability — The biometric can be collected in a reasonably easy fashion for quick identification.
- Performance — The degree of accuracy of identification for the biometric must be quite high before the system is considered operational.
- Acceptability — The collection and use of the biometric is publicly accepted.
- Resistance to circumvention — Collection and use of the biometric is harder to circumvent than other identification systems.

When deciding which biometric to collect and use, these seven measures provide a baseline for making an informed choice. The collection or exploitation technology available must also be considered in conjunction with these seven measures to determine operational utility. A modality may provide a high degree of accuracy, but without technology that can be used in a tactical environment, it will do us no good. The selection of fingerprints, iris images, and facial photos were driven by the technology available at the time of collection system deployment and remains valid.

Tactical Considerations for Modality Selection

Tactical considerations will also impact on the choice of biometric modalities. During an initial biometric's enrollment of an individual, as many biometrics as possible should be collected consistent with the mission and enemy situation. Theater policies set guidance on "full enrollment" (normally face, both irises, and all ten fingerprints — slapped and rolled if possible) versus "hasty enrollment" (normally face, irises, forefingers, and thumbs). If encountering an individual for the first time, it is absolutely essential that at least some fingerprints (preferably rolled prints) be taken, as only these will provide the means for connecting individuals to fingerprints collected forensically from IED components. If the mission calls for verifying the identity of previously enrolled individuals for base access or population-management purposes, then iris-only collection may be an acceptable option, particularly if speed is required.

Biometrics Enrollment		Collection Platforms	
Fingerprint		Handheld Interagency Identity Detection Equipment (HIIDE)	
Picture		Biometric Automated Toolset (BAT)	
Iris Scan		Secure Electronic Enrollment Kit (SEEK) and Cogent Fusion	
Personal Data		Afghan Crossmatch Jump Kits	

Figure A-1. Enrollment and collection platforms

Fingerprint recognition has long been used by law enforcement and provides a good balance related to the seven measures of biometrics. Nearly every human being possesses fingerprints (universality) with the exception of hand-related disabilities. In Afghanistan, however, a lifetime of hard work has all but eradicated some fingerprints on local farmers. They present something of a challenge, but there should be some readable prints on a standard ten-print card. Fingerprints are distinctive and fingerprint details are permanent, although they may temporarily change due to cuts and bruises on the skin or external conditions (e.g., wet fingers). Live-scan fingerprint sensors can quickly capture high-quality images (collectability). The deployed fingerprint-based biometric systems offer good performance, and fingerprint sensors have become quite small and affordable. In some societies, fingerprints have a stigma of criminality associated with them, but that is changing with the increased demand of automatic recognition and authentication in a digitally interconnected society (acceptability). By combining the use of multiple fingers, cryptographic techniques, and “liveness” detection, fingerprint systems are becoming quite difficult to circumvent. Fingerprints used in tactical biometric collections provide a direct link to battlefield forensics and the latent prints of value collected from pre- and post-blast forensic collections, cache sites, safe houses, and anywhere else a person has been. When seeking bomb makers, emplanters, or other “forensically interesting” individuals, fingerprints are the biometric of choice.

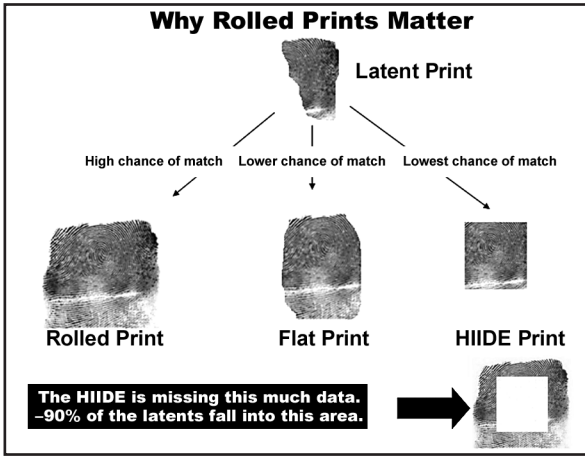


Figure A-2. Why rolled fingerprints matter

Iris image

The iris is the externally visible, colored ring around the pupil of the eye. It is a physical feature of a human being that can be recorded and then used for biometric verification or identification. The human iris is well protected, and even though it is externally visible, it is an internal part of the eye. Iris patterns are both highly complex and unique (the chance of two irises being identical is estimated at 1 in 10 to the 78th power), making them very well suited for biometric identification. While not as prevalent as fingerprint databases, iris image databases are growing at a rapid rate. However, iris image databases can be searched much faster than fingerprint databases, allowing very fast verification or identification. Several countries now use iris recognition technology to speed access through customs.

Iris recognition performs very well against the seven measures of biometric effectiveness. All humans (including blind people) possess irises (universality) with some exceptions (e.g., people with aniridia, which is the absence of an iris). Iris patterns are scientifically proven to be distinctive. Patterns are also permanent from infancy to old age, with the exception of the effects of some eye diseases. Existing sensors can capture high-quality images (collectability), although several trials may be necessary. The iris recognition system offers excellent performance, even in identification mode with huge databases of enrolled users. The acceptability of iris recognition is relatively low but growing. Finally, while the first systems were once easy to fool with a picture of an iris placed at the appropriate distance, new systems are more expensive but quite difficult to circumvent. Iris images are unsuitable for finding bomb makers or emplacers but are

ideal for verifying the identities of previously enrolled individuals at checkpoints or during population management patrols.

Face

The face is an obvious choice for a biometric, as it is the physiological characteristic used every day by humans to identify others. Face recognition is considered less invasive than other biometrics and generally has a higher level of user acceptance. However, it is also more challenging technologically — no computer matches the human brain when it comes to face recognition. Face recognition has lower accuracy rates than other biometric modalities, such as iris or fingerprint recognition. Face recognition does well in the areas of universality (everybody has a face), collectability (2D face recognition uses a photograph, which is easy to acquire), and acceptability (people are accustomed to the idea of using the face for identification and the technique is nonintrusive). It struggles with distinctiveness (the patterns of faces show less variation compared to fingerprints or irises for example), permanence (faces change significantly over time and can be surgically altered), and performance (currently face recognition has much lower accuracy rates than the other featured biometric technologies). Face recognition's resistance to circumvention depends on the application. It is not possible to spoof a face recognition system in the way a latex fingerprint might spoof a fingerprint system, but the low accuracy rates of face recognition make it easier for impostors to be falsely accepted.

One aspect of face collection that makes it somewhat unique is that it is possible to match a high-quality facial image collected during a biometrics enrollment to another facial image collected for a non-biometric-related mission. For example, it may be possible to biometrically match against a high-quality handheld photo taken during a patrol, leadership engagement, or any other photo opportunity. Thus, ensuring facial photos are part of the biometrics enrollment opens up a wide range of matching opportunities to non-biometric collections.

Biometrics Technology

All biometrics collections systems work off the same basic process of collecting a biometric sample, processing the image, and creating a template that is stored for later reference, along with whatever contextual information we wish to link to the collection. In some cases, a copy of the raw image is stored, but that may not be necessary based on which modality is used.

To identify a person based on a submitted biometric, the process is much the same as the collection without needing to immediately store the template or related data. The submitted template is matched against a specific template in a database, when the person is providing a claimed identity, or matched

against all templates when the identity of the person is unknown. If a match is (or is not) made, then a decision is made based on why the biometric was submitted. When matching a fingerprint against a watch list, receiving “no match” results means the person hasn’t been identified for further scrutiny. When matching an iris against a base access roster, a positive match means the person will be allowed access.

The two most prevalent biometrics collections systems in use in Afghanistan are the Biometrics Automated Toolset (BAT) and the Handheld Interagency Identity Detection Equipment (HIIDE). These systems are available as theater-provided equipment and can also be requested for use in situational training exercises in preparation for deployment.

The BAT system is made up of a ruggedized laptop computer, BAT software, fingerprint scanner, iris image collection device, and a camera. It is a multimodal system (collects and matches against more than one biometric) used to collect, match, transmit, and store biometrics and related contextual data. It can be used to identify and track persons of interest and to build digital dossiers on individuals that include interrogation reports, biographic information, and relationships. The database of information and biometrics are shared throughout the theater, and much of the data can be shared with other federal agencies.

The HIIDE is the primary collection tool for biometrics in a tactical environment and is a tactical extension of BAT. It can collect the same three modalities as the BAT system, but due to size and processing power, does not have the same database and connectivity capabilities as the BAT. This is the primary device used for enrollments in Afghanistan based on its portability (2.3 pounds) and the challenges of the rugged environment. The HIIDE is used to enroll and establish the identity of persons of interest in forward deployed sites, on objectives, or any other time coalition forces desire to check a person’s claimed identity.

Appendix B

Training

Introduction

This appendix will focus on biometrics training in terms of who needs what training and how to access it. Biometrics plays an increasingly important role in counterinsurgency operations. Focused predeployment training is critical to achieving operational effects with biometrics as soon as possible once a unit arrives in theater. However, with biometrics training, as with many other things, one size does not fit all.

Who Needs Biometrics Training?

Per U.S. Army Forces Command training guidance, commanders, leaders, staffs, and Soldiers all require training on biometrics and biometric collection systems. However, not everyone needs the same type of training. Units should work with capabilities integration team representatives in their areas and the other training contacts listed at the end of this appendix to match their training requests to the requirements of their deployment missions.

Commanders, leaders, staff officers, and noncommissioned officers (NCOs) of units that will employ biometric systems should receive a briefing on the impact of biometrics and its incorporation into the military decisionmaking process. It is critical that leaders understand the variety of missions that biometrics supports and that the various staff sections also understand their roles in biometrics mission support.

Among the most important staff and leader tasks is the selection of the right Soldiers to receive training on biometrics operation and collection equipment and the continued use of those trained personnel in biometrics-related jobs. This, in itself, builds unit expertise and experience to optimize the use of biometrics.

Types of Training Available

There are several courses available for training at a unit's home station. These include courses offered by the mobile biometrics training team (MBTT), local counter improvised explosive device centers, and battle command training centers. Biometrics training is also available at the combat training centers (CTCs) and at some mobilization training centers (MTCs). It is also offered after deployment in Afghanistan. However, many units have passed the lesson that receiving biometrics training at the CTC is almost too late. Many report this training should be conducted at the unit's home station prior to deploying to a CTC.

Training offered by the biometrics new equipment training team includes:

- **Biometrics for Commanders, Leaders, and Staffs Course (1 Hour):** Provides leaders with the skills and knowledge necessary to incorporate tactical biometric systems into staff planning and operations. Training focuses on specific commander, leader, and staff tasks that maximize the use of the systems and enhance operations. Course also discusses actions by staffs during assessment, planning, and operations.
- **Biometrics Operations Specialist Course (40 Hours):** Provides operationally focused training on the use of Biometrics Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE), plus advanced instruction on planning, techniques, and procedures for biometrics support of unit missions. The course is designed for Soldiers assigned to company-level intelligence support teams, for officers and senior NCOs working on the brigade or battalion intelligence and operations staffs, or other positions that require an in-depth knowledge of biometric operations and mission support. Individuals completing this course should be able to advise the commander and staff on the effective employment of biometrics in support of unit missions, plan for and supervise biometrics support, ensure timely and appropriate movement of biometrics data, and train Soldiers to use unit-level biometrics equipment. This individual will serve as the focal point for biometrics training and operations in the unit, so the individual's skill and knowledge should go beyond the basic use of biometrics equipment.
- **Basic Biometrics Operators Course (16 Hours):** Provides Soldiers with the skills and knowledge necessary to operate the BAT system to perform biometric enrollment and identification, manage the local BAT database, transfer data between BAT and HIIDE, screen locally employed personnel, operate biometrically enabled entry control points, and use biometrics in support of human terrain mapping and force protection.
- **HIIDE with BAT Overview (8 Hours):** Provides service members with the skills and knowledge necessary to enroll and identify with the HIIDE and also provides an overview of BAT. Training focuses on the use of HIIDE in route clearance and census operations and on the transfer of collections from HIIDE to BAT.
- **HIIDE Course (4 Hours):** Provides service members with the skills and knowledge necessary to use HIIDE on patrols, at checkpoints, and in other operations involving enrollment and/or identification with the HIIDE.

Other Available Training:

- **National Ground Intelligence Center (NGIC) Biometrics-Enabled Intelligence Course:** Provided by the NGIC, this “on request” training is provided by a mobile training team and focuses on intelligence analysts. The training provides analysts the necessary skills and understanding of the tools to draw upon biometric intelligence products during the analysis process.
- **Combat Training Center (CTC) Biometrics Refresher Training (HIIDE, 1.5 Hrs; BAT, 8 Hrs):** Covers BAT and HIIDE enrollment and identification, data upload/download between BAT/HIIDE, and creating tracking reports. If the trainee attended biometrics training at home station, this will be a review that builds on existing skills and knowledge.
- **Biometrics Training at 1st Army Mobilization Training Centers (MTCs):** The training coordinator at the MTC works with units to determine their biometrics training needs. Based on mission analysis and availability of time; training ranges from 1–2 hour familiarization to the Biometrics Operations Specialist Course.
- **Task Force Biometrics Training (in Afghanistan):** Task Force Biometrics is developing a comprehensive and detailed training plan for units that have deployed to theater. Task Force Biometrics currently has MBTTs and contract trainers available to train U.S. and coalition members on the use of biometric collection tools. Units should contact Task Force Biometrics to arrange training at their location.

What Every Soldier Should Know About Biometrics

Every Soldier should receive a basic orientation on biometrics. At the end of that orientation, which can be accomplished in an hour (or a little more if it includes an equipment demonstration), the Soldier should be able to do the following:

- Define biometric and biometrics.
- Define enrollment, identification, and verification.
- List which biometrics are used by the Department of Defense (DOD) and which biometrics are the most and least accurate.
- Identify the three biometric enrollment/identification systems most commonly used by U.S. forces in theater.
- Describe how biometrics collected by Soldiers get into the DOD biometrics database.

- List three reasons why quality collections are critically important.
- Explain the difference between a watch list and a positive access roster and how each is used.

Training Point of Contact:

United States Army Intelligence Center of Excellence (USAICoE)
New Systems Training and Integration Division
Commercial Phone: (520) 538-0706
NSTIO@CONUS.ARMY.MIL
<<https://ikn.army.mil/apps/g3mtt/>>

Appendix Checklist (1) Biometrics Unit Checklist

Unit: _____ NCOIC/OIC: _____ Location: _____ Date: _____

Entry Control Point (ECP) Operations

- HIIDE is present at the ECP.
- At least one service member trained on the HIIDE present at all times.
- HIIDE's biometrics enabled watch list (BEWL) and local population set are no older than 12 hours.
- ECP NCOIC has established and is enforcing a unit standing operating procedure (SOP) that supports theater standards for a biometrically enabled ECP.
- Anyone NOT a U.S. service member, or U.S. contractor will be processed using HIIDE. (**Note:** We do not enroll coalition members.)
- Tracking report is filled out on anyone entering the ECP who is already in the HIIDE.
- HIIDE should be rotated out by the sergeant of the guard at least every 12 hours to assure a current BEWL and fresh batteries.

Tactical Operations

- HIIDE has the current BEWL and is present on all patrols/operations outside the forward operating base (FOB).
- At least two personnel trained on the HIIDE are present on the patrol/operation outside the FOB.
- HIIDE's BEWL is no older than 12 hours (from the time of departure).
- HIIDE's batteries are fully charged at the beginning of the patrol (two batteries per eight hours).
- All military-aged males on the objective will be processed using HIIDE/BAT (time dependent).
- A tracking report is filled out on personnel who are already in the HIIDE.
- Tactical enrollment (enrollment using the HIIDE) is completed for personnel who are not already in the HIIDE.
- All deceased individuals will be processed using HIIDE for identification purposes only. If deceased is in the HIIDE, the Soldier/Marine will complete a tracking report.

Company Intelligence Support Team (COIST) Role

- BAT/HIIDE and all peripheral equipment will be maintained at the COIST when not required for missions.
- COIST will update the HIIDE with current BEWL per SOP prior to starting the prebrief.
- COIST will issue HIIDE as a part of the mission prebrief.
- COIST will ensure the HIIDE is fully charged prior to the prebrief.
- COIST will ensure the HIIDE is fully functioning prior to prebrief (preventive maintenance checks and services).
- COIST will provide recommended employment of the HIIDE as a part of its prebrief (collections/identity management/force protection).
- COIST will collect the HIIDE as a part of the debriefing process.
- COIST will download any new information from the HIIDE to the BAT database after the debriefing process is complete and send/report enrollments/tracking reports/relationships to higher headquarters.
- COIST should fully utilize the biometric intelligence resource (BIR), Tactical Ground Reporting Network, AxisPro, and other analytic methods to turn the raw data into actionable intelligence for the commander.

Appendix Checklist (2)

Biometrics Relief in Place/Transfer of Authority Checklist

Unit: _____ NCOIC/OIC: _____ Location: _____ Date: _____

- How many BAT/HIIDE?
- Location of all BAT/HIIDE?
- What locations are connected by SECRET Internet Protocol Router Network (SIPRNET) to BAT server?
- Passwords for BAT/HIIDE devices?
- Internet protocol address settings for HIIDE/BAT if applicable?
- What are the device settings on HIIDE (if applicable)?
- What are the contact numbers and e-mail for field service engineer support?
- What is the contact information for the Combined Joint Task Force (CJTF)–101 biometric management office?
- Are local databases maintained on BAT kits that are not connected to the network?
- What are the naming conventions and search criteria for the local databases?
- What is the SOP for turn-in and repair of defective BAT/HIIDE equipment?
- How are you employing biometrics within the area of operations?
- What locations have badge printing capability?
- How do service members navigate to the file transfer protocol (FTP) site to upload their BAT/HIIDE biometric data files (BDFs)?
- How do service members download the current CJTF–101 biometric watch list?
- How are BDF collections moved from locations that have no SIPRNET connectivity?
- How many “local alerts” do you have currently placed in the BAT database?

- Are there maintenance and serviceability issues with the BAT and HIIDE devices?
- Is the current watch list provided on disk to locations with no SIPRNET connectivity?

Appendix Checklist (3) Biometrics Entry Control Point Checklist

Location: _____ Date: _____

Entry Control Point (ECP) Operations

- BAT or HIIDE is used to vet individuals against the watch list.
- BAT or HIIDE is used to vet individuals with a positive control database.
- ECP wired with SIPRNET, and BAT is used to vet subjects against the entire BAT database (preferred).
- Biometrics is being used during base perimeter operations as a force protection measure.
- All local nationals and third country nationals requesting base access are biometrically enrolled.
- Biometrics, not badges, are being used to verify identity at ECPs.
- Badges that comply with the theater template are used to verify access, escort requirements, and privileges.

Connectivity

- Location has SIPRNET for uploading biometric collections to the Smart FTP site or directly to the BAT database.
- Location has connectivity to support downloading the watch list from the designated Smart FTP site.

Download/Upload Stations

- Unit employs proper tactics, techniques, and procedures (TTP) for uploading watch list and/or positive control database to the HIIDE.
- Unit uploads watch list to their HIIDEs at a minimum weekly.
- Unit employs proper TTP to upload new enrollments from HIIDE to the Smart FTP site or to the BAT database.
- Unit uploads new enrollments at a minimum weekly to the Smart FTP site or to the BAT database.
- If no or poor SIPRNET connectivity, unit has TTP to upload watch list and download collections to an offsite SIPRNET location.

Watch List Updates

- Unit uses the Smart FTP site to download watch list.
- Unit receives update of refreshed watch list posting.
- Unit has TTP for reacting to a watch list hit.
- Unit knows how to create a local alert and understands that local alerts expire after a specific number of days.
- Unit knows how to nominate an individual to the ISAF watch list.
- Unit is receiving watch list and weekly updates via SIPRnet email or they know where to download them.

TTP Compliance

- Unit understands TTP for proper biometric collection.
- Unit understands standard for quality enrollments (i.e., photographs, two irises, and 10 properly rolled/pressed fingerprints).
- Unit has TTP for routinely checking the quality of biometric enrollments.
- Unit uploads as attachments all information gathered from base access screening.
- Unit uses tracking reports to make watch list updates or nominations for access ban.

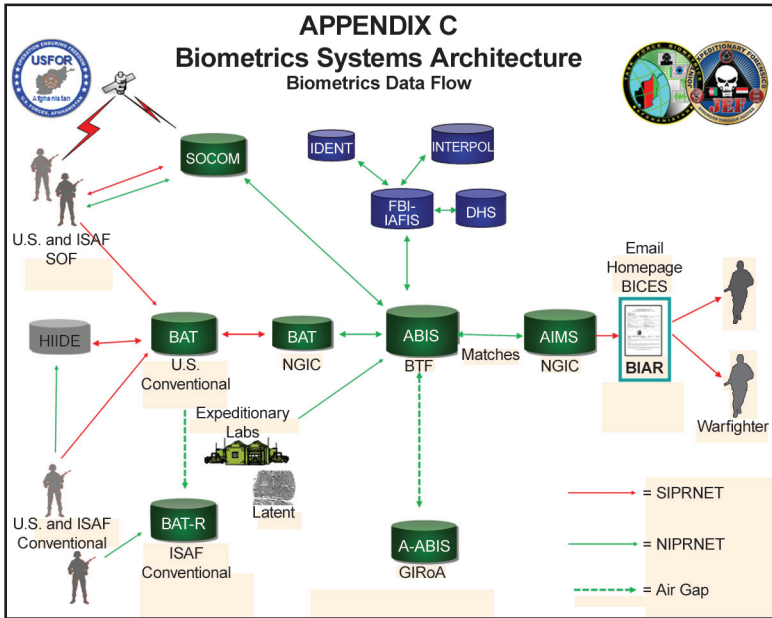
Equipment/Training Requests

- Biometric equipment is in good working order — no missing or broken components or parts.
- Unit has sufficient biometric equipment on hand for mission requirements.
- Unit understands how to request equipment, technical support, and training.
- Unit has requirements that need the immediate attention of the regional command biometrics support element.

Comments: _____

Appendix C

Biometrics Systems Architecture



Legend:

A-ABIS: Afghanistan Automated Biometrics Identification System
 ABIS: Automated Biometrics Identification System
 AIMS: Automated Identification Management System
 BAT: Biometrics automated toolset
 BAT-R: BAT-Releasable
 BIAR: Biometric identification analysis report
 BICES: Battlefield Information, Collection and Exploitation System
 BTF: Biometrics Task Force
 DHS: Department of Homeland Security
 FBI-IAFIS: Federal Bureau of Investigation Integrated Automated Fingerprint Identification System

GIROA: Government of the Islamic Republic of Afghanistan
 HIIDE: Handheld Interagency Identity Detection Equipment
 IDENT: DHS' Automated Biometric Identification System
 INTERPOL: International Criminal Police Organization
 ISAF: International Security Assistance Force
 NGIC: National Ground Intelligence Center
 NIPRNET: Nonsecure Internet Protocol Router Network
 SIPRNET: SECRET Internet Protocol Router Network
 SOCOM: Special Operations Command
 SOF: Special operations forces

Appendix D

Biometrics Glossary

– A –

Analyze	Convert data to actionable information and recommendations as applicable to increase situational awareness and better understand possible courses of action.
Armed Forces DNA Identification Laboratory (AFDIL)	Provides scientific services in the field of forensic DNA analysis to the Department of Defense (DOD) and other agencies, as well as worldwide, and DNA reference specimen collection, accession, and storage of United States military and other authorized personnel.
Associated information	Nonbiometric information about a person. For example, a person's name, personal habits, age, current and past addresses, etc.
Attempt	The submission of a single set of biometric samples to a biometric system for identification or verification.
Authoritative source	Primary DOD-approved repository of biometric information on a biometric subject.
Automated Fingerprint Identification System (AFIS)	A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records to determine the identity of an individual.
Automated Identification Management System (AIMS)	A system that acts as a central web-based informational portal between U.S. Central Command (USCENTCOM), National Ground Intelligence Center (NGIC), and the biometrics fusion center (BFC) that is designed to fuse intelligence analysis and value added comments from field users of matched biometric and biographic data.

– B –

Biometrics enterprise core capability (BECC)	Multimodal, multifunctional successor to ABIS; a comprehensive system that includes multidomain biometrics collection, storage, and matching.
Behavioral biometric characteristic	A biometric characteristic that is learned and acquired over time rather than one based primarily on biology.
Biographic data	Data that describes physical and nonphysical attributes of a biometric subject from which a biometric sample data has been collected.
Biological biometric characteristic	A biometric characteristic based primarily on an anatomical or physiological characteristic rather than a learned behavior.
Biometric	Of or having to do with biometrics.
Biometric application decision	A conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores, and possibly other nonbiometric data.
Biometrics Automated Toolset (BAT)	A multimodal biometric system that collects and compares fingerprints, iris images, and facial photos.
Biometric capture device	Device that collects a signal from a biometric characteristic and converts it to a captured biometric sample.
Biometric capture process	A process of collecting or attempting to collect signals from a biometric characteristic and converting them to a captured biometric sample.
Biometric characteristic	A biological and behavioral characteristic of a biometric subject that can be detected and from which distinguishing features can be extracted for the purpose of automated recognition of biometric subjects.

Biometric data	A catch-all phrase for computer data created during a biometric process. Biometric data is used to describe the information collected during an enrollment, verification, or identification process.
Biometric database	A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related biometric subject information, etc.
Biometric encounter	A biometric encounter occurs when a biometric sample(s) is captured from an individual or a latent biometric sample(s) is collected.
Biometric feature	Numbers or labels extracted from biometric samples and used for comparison.
Biometric file	The standardized individual data set resulting from a collection action. The biometric file is composed of the biometric sample(s) and contextual data (biographic data and situational information)
Biometric Identification System Access (BISA)	A biometric and contextual data collection and credential card for production system.
Biometric identity	A biometric identity is established when a biometric sample(s) is used instead of a name to identify a person of interest (POI).
Biometric information	A catch-all phrase that includes but is not limited to biometric data, contextual data, and associated information obtained during the biometric process.
Biometric intelligence analysis report (BIAR)	BIARS are first-phase analytical products that provide current intelligence assessments on individuals who have been biometrically identified at least once and who may pose a threat to U.S. interests.

Biometric intelligence resource (BIR)	A system that ingests biometric signatures and contextual data collected from DOD biometric processing systems and makes this information available to members of the worldwide intelligence community through a web-based interface for the purpose of positive identification of individuals and tracking related intelligence.
Biometric model	Stored function (dependent on the biometric data subject) generated from a biometric feature(s).
Biometric property	The descriptive attributes of the biometric subject estimated or derived from the biometric sample by automated means.
Biometric record	Data record containing biometric data.
Biometric reference	One or more stored biometric samples, biometric templates, or biometric models attributed to a biometric subject and used for comparison.
Biometric sample collector	An individual performing the biometric sample collection.
Biometric subject	An individual from which biometric samples are collected.
Biometric system	Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system.
Biometric template	Set of stored biometric features comparable directly to biometric features of a recognition biometric sample.
Biometrics enabled physical access	The process of granting access to installations and facilities through the use of biometrics.
Biometrics enabled watch list (BEWL)	Any list of POI, with individuals identified by (BEWL) biometric sample instead of by name and the desired/recommended disposition instructions for each individual.

Biometrics	A general term used alternatively to describe a characteristic or a process.
Biometrics program	All systems, interfaces, acquisition programs, processes, and activities that are utilized to establish identities of people through the use of biometrics modalities.
Biometrics-enabled intelligence (BEI)	Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist/insurgent network and related pattern analysis, facilitates high-value individual targeting, reveals movement patterns, and confirms claimed identity.

– C –

Collect	The capability and/or process to capture biometric sample(s) and related contextual data from a biometric subject, with or without his knowledge.
Comparison	Process of comparing a biometric reference with previously stored references in order to make an identification or verification decision.
Comparison decision	Determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies), including a threshold, and possibly other inputs.
Contextual data	Elements of biographic data and situational information (who, what, when, where, how, why, etc.) associated with a collection event and permanently recorded as an integral component of the biometric file.

– D –

Decide/Act	The response by the operational or business process owner (either automated or human in-the-loop) to the results of the match and/or analysis.
Defense Biometrics Identification System (DBIDS)	A DOD system developed by the Defense Manpower Data Center (DMDC) as a force protection program to manage installation access control for military installations.
Deoxyribonucleic acid (DNA) matching	Utilizing DNA to identify a biometric subject.
Detainee Reporting System (DRS)	A system designed to support the processing of prisoners of war and detainees.
DNA profile	The results of DNA analysis, which determines the relative positions of DNA sequences at several locations on the molecule.
DNA sample	A collection of DNA molecules that can be quantified, amplified, separated, and analyzed.
DNA source	The individual or material from which a DNA sample can be collected or extracted.
DOD Automated Biometric Identification System (DOD ABIS)	DOD ABIS is the central, authoritative, multimodal biometric data repository.
DOD electronic biometric transmission specification (DOD EBTS)	DOD EBTS is a transmission specification to be used between DOD systems that capture biometric data and repositories of biometric data.

– E –

Electronic fingerprint transmission specification (EFTS)	A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS).
--	---

Enroll	Create and store, for a biometric subject, an enrollment data record that includes biometric reference(s) and, typically, nonbiometric data.
Enrollment	Process of collecting a biometric sample from a biometric subject, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

– F –

Face recognition	A biometric modality that uses an image of the visible physical structure of a biometric subject's face for recognition purposes.
False acceptance	When a biometric system incorrectly identifies a biometric subject or incorrectly authenticates a biometric subject against a claimed identity.
False match	The comparison decision of "match" for a recognition biometric sample and a biometric reference that are not from the same source.
False non-match	A comparison decision of "no-match" for a recognition biometric sample and a biometric reference that is from the same source.
False rejection	The failure of a biometric system to identify a biometric subject or to verify the legitimate claimed identity of a biometric subject.
FBI electronic biometric transmission specification (FBI EBTS)	The FBI EBTS specifies the file and record content, format, and data codes necessary for the exchange of fingerprint, palm print, facial, and iris information between federal, state, and local users and the FBI.
Fingerprint	Image left by the minute ridges and valleys found on the hand of every person. In the fingers and thumbs, these ridges form patterns of loops, whorls, and arches.
Fingerprint recognition	Biometric modality that uses the physical structure of a biometric subject's fingerprint for recognition purposes.

Fingerprint scanning	Acquisition and recognition of a biometric subject's fingerprint characteristics for identification purposes.
Flat fingerprint	Fingerprints taken in which the finger is pressed down on a flat surface but not rolled; also known as plain fingerprint.
Forensic	Relates to the use of science or technology in the investigation and establishment of facts or evidence.
Forensics	The application of multidisciplinary science capabilities to establish facts.
Friction ridge	The ridges present on the skin of the fingers and toes and on the palms and soles of the feet that make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints.
Full enrollment	Enrollment of biometric data on a subject that includes 14 fingerprint images (four slaps, 10 rolls), five face photos, two irises, and required text fields. The sample must be EBTS compliant.

– G –

Gait	A biometric subject's manner of walking.
------	--

– H –

Hand geometry recognition	A biometric modality that uses the physical structure of a biometric subject's hand for recognition purposes.
Hand scan	Print from the outer side of the palm.

– I –

Identification	The one-to-many (1:N) process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the biometric subject whose template was matched.
Identity	A set of characteristics by which an entity (e.g., human, application, device, service, or process) is recognizable from every other entity.
Identity assurance	The capability to affix, verify, and/or determine the identity of a person (living, deceased, unconscious, nonfunctioning, uncooperative, or unaware), an organization, or entity.
Identity claim	A statement that a biometric subject is or is not the source of a reference in a database.
Identity dominance	The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity and/or to counter biometric technologies and processes.
Identity facilitation	The capability to plan, organize, lead, coordinate, and control the use of resources to deliver accurate, complete, secure, and timely identity information products and services to operational users on demand.
Identity integration	Identity integration highlights the capability of services, combatant commands, government agencies, international and national organizations, and associated systems, resources, and entities to cooperate and interoperate as needed to deliver identity assurance, identity protection, and identity facilitation products and services to support warfighter/user operations.
Identity intelligence	Information produced by the discovery, management, and protection of identity attributes in support of U.S. national security interests.

Identity management	A business function that authenticates a biometric subject to validate identity, DOD affiliation, and authorization of the biometric subject.
Identity protection	The process of safeguarding and ensuring the identities of individuals, devices, applications, and services are not compromised.
Identity superiority	The management, protection, and dominance of identity information for friendly, neutral or unknown, and adversary personnel.
Individual	As used in the biometrics enterprise, an individual refers to a single human being.
Integrated Automated Fingerprint Identification System (IAFIS)	The FBI's large-scale 10 fingerprint (open-set) identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses.
Iris recognition	Biometric modality that uses an image of the physical structure of a biometric subject's iris for recognition purposes.
– K –	
Keystroke dynamics	A potential biometric modality that uses the cadence of a biometric subject's typing pattern for recognition.
– L –	
Latent fingerprint	A fingerprint "image" left on a surface touched by a biometric subject.
Latent print	Transferred impression of friction ridge detail not readily visible; generic term used for questioned friction ridge detail.

Latent sample	A biometric residue that is dormant, inactive, or nonevident but can be captured, measured, and stored.
Live capture	Fingerprint capture technique that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface).
Live scan	Occurs when taking a fingerprint or palm print directly from a biometric subject's hand.
Liveness detection	A technique used to ensure that the biometric sample submitted is from a living biometric subject.
Local trusted source	A sub-set of the authoritative source and is established to accomplish a specific function within an operational mission or business process.
Local untrusted source	A local repository of biometric files that that have not been enrolled with an authoritative or local trusted source.

– M –

Manage	The capability and/or process to perform administrative duties related to biometrics.
Match	Comparison decision that the recognition biometric sample(s) and the biometric reference are from the same source. Also, the capability and/or process to compare biometric data to link previously obtained biometrics and related contextual data to a particular identity for identification or verification of identity.
Mimic	The presentation of a biometric sample in an attempt to fraudulently impersonate someone other than the biometric subject.
Modality	A type or class of biometric sample originating from a biometric subject.

Mug shot A photograph of an individual's face. Interchangeable with facial image.

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

– N –

Non-match Comparison decision that the recognition biometric sample(s) and the biometric reference are not from the same source.

Nuclear DNA (nDNA) The DNA contained within the nucleus of a cell.

– O –

One-to-many Comparing one biometric reference to many biometric references to identify a biometric subject; sometimes referred to as 1:N.

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

– P –

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

Person of interest (POI) An individual for whom information needs or discovery objectives exist.

Personally identifiable information (PII) Information about an individual that identifies, links, relates, or is unique to or describes him or her (e.g., a social security number or age).

Plain fingerprint Fingerprints taken in which the finger is pressed down on a flat surface but not rolled; also known as flat fingerprint.

Platen The surface on which a finger is placed during optical finger imaging.

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

– R –

Recognition A generic term used in the description of biometric systems (e.g., face recognition or iris recognition) relating to their fundamental function.

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

Reference The capability and/or process of querying various repositories of associated information on individuals (intelligence, medical, human resources, financial, security, education, law enforcement, etc.) for analysis purposes.

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

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

– S –

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

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

Share	The capability and/or process to transfer (send and/or receive) biometric sample(s), contextual data, and/or associated information within the DOD and between DOD and other national, international, and nongovernmental organizations as appropriate.
Signature dynamics	A behavioral biometric modality that analyzes dynamic characteristics of a biometric subject's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.
Situational information	The who, what, when, where, how, why, etc. associated with a collection event and permanently recorded as an integral component of contextual data.
Slap fingerprint	Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card.
Source	An approved database and infrastructure that stores biometrics files.
Speaker recognition	A biometric modality that uses a biometric subject's speech, a feature influenced by both the physical structure of a biometric subject's vocal tract and the behavioral characteristics of the biometric subject, for recognition purposes.
Speech recognition	A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology.
Store	The capability and/or process of enrolling, maintaining, and updating biometric files to make available standardized, current biometric sample(s) and contextual data on biometric subjects when required.
Submission	The process whereby a subject provides a biometric sample to a biometric system.

– T –

Tactical enrollment	Enrollment of biometric data on a subject that includes at least two fingerprints (indexes), two iris prints, and required text fields. The sample must be EBTS compliant.
Ten (10) print match or identification	An absolute positive identification of a biometric subject by corresponding each of their 10 fingerprints to those in a system of record.
Terrorist watch-list person data exchange standard (TWPDES)	A data exchange format for terrorist watch list data that supports the Department of State, Department of Justice, intelligence community under the Director of Central Intelligence, and the Department of Homeland Security to develop and maintain, to the extent permissible by law, the most thorough, accurate, and current information possible about individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism.
Tethered Biometric System	Use of biometric sensors between deployed personnel within a robust command and control architecture.
Threshold	A user setting for biometric systems operating in the verification or open-set identification (watch list) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold.
Transaction	A command, message, or input record that explicitly or implicitly calls for a processing action. Information contained in a transaction shall be applicable to a single subject.

– U –

U.S. visitor and immigrant status indicator technology (US-VISIT)	Using biometrics, such as digital, inkless finger scans, and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure the person crossing the U.S. border is the same person who received the visa.
United States Army criminal investigation laboratory (USACIL)	USACIL provides forensic laboratory services to DOD investigative agencies and other federal law enforcement agencies.
Untethered Biometric System	Collection, analysis, and use of biometric sensors between deployed personnel outside of a robust command and control architecture.

– V –

Verification	The one-to-one process of matching a biometric subject's biometric sample against his stored biometric file; also known as authentication.
--------------	--

Appendix E

Biometrics References

The following are some Web resources that pertain to biometrics and biometrics-enabled intelligence. The primary reference for biometrics training and deployment guidance can be found on the Center for Army Lessons Learned (CALL) restricted website <<https://call2.army.mil/toc.aspx?document=2398#2c>> under:

FORSCOM Predeployment Training Guidance for Follow-On Forces Deploying to ISO Southwest Asia (SWA) Change 5.

Note: Department of Defense (DOD) service members and civilians can access the CALL website with a valid common access card (CAC). Personal computer users will need to install the DOD root certificate to use this login option. (For information on the DOD root certificate, go to <https://help.us.army.mil/cgi-bin/akohd.cfg/php/enduser/std_adp.php?p_faqid=50>).

For contractors, other services (U.S. Marine Corps, U.S. Air Force, U.S. Navy and U.S. Coast Guard), and other government services, a CALL-supplied user name/password must be obtained. This process is started by submitting a CALL request for information at <<https://call2.army.mil/rfi/>>.

The other principal websites for biometrics are:

Biometrics.Gov	< http://www.biometrics.gov >
Biometrics Identity Management Agency (BIMA)	< http://www.biometrics.dod.mil >

Appendix F

Special Operations Biometrics

During a mission, a special operations forces (SOF) team collects letters announcing any citizen supporting U.S. forces would be killed. Upon returning to the forward operating base, the team turns in the documents to the exploitation analysis center (EAC). Latent prints are extracted from the letters and submitted to the identity operations portal along with digital copies of the letters. Within a day, the latent prints match to an identity, and the information is immediately passed to the teams and Combined Joint Special Operations Task Force–Afghanistan (CJSOTF–A). The U.S. Special Operations Command (USSOCOM) biometric analysis and coordination cell (BACC) is able to develop a biometric tracking information package (BTIP) with link analysis of known associates of the person identified, to include photos and geospatial information of possible locations of the individual. Additionally, the BACC coordinates the person being placed on the biometrics enabled watch list. The SOF team is able to target the individual, capture him, and conduct SOF site exploitation (SSE) of the individual's residence. The team uses its Secure Electronic Enrollment Kit (SEEK) to collect the individual's biometrics and confirm his identity. Biometrics are collected on other persons on target and sent to the exploitation Web application for matching. Within 15 minutes, the team is able to confirm that one of these individuals is a Level 4 watch list hit, a former detainee. This individual is identified to be detained for further questioning. Based on information provided by the BACC, tactical questioning is effective. The items collected on target, to include latent images, improve the analysis of associates and leads to additional targeting.

Identity Operations

SSE consists of biometrics, forensics, and documentation and media exploitation (DOMEX). This appendix will focus on theater SOF biometric operations in Afghanistan. SOF teams normally operate as a detachment assigned to the CJSOTF with specific missions and areas of interest. These elements will consist of Army, Marine, and Navy SOF teams. SOF biometric capabilities, at the team level, currently allow them to submit biometric collections to the DOD Automated Biometric Identification System (ABIS) and receive a match/no match response in less than 15 minutes. This timely response also includes some metadata about the previous encounters that helps the SOF user decide and react to the person of interest.

SOF teams use live-scan devices and fingerprint cards for the collection of live biometrics. Teams will collect latent fingerprints, or items with potential latent prints, or DNA as part of SSE. Army SOF employs its Special Forces

Group chemical decontamination detachments to operate the EACs for the collection of forensically derived biometrics, such as latent fingerprints and DNA. The EACs also provide exploitation of DOMEX and trace evidence linked to the biometrics collected.

Architecture

SOF uses a web-based architecture, over either Nonsecure Internet Protocol Router Network (NIPRNET) or SECRET Internet Protocol Router Network (SIPRNET), to facilitate the quickest response from the ABIS. SOF files are also searched against the Department of Justice's Integrated Automated Fingerprint Identification System, Department of Homeland Security's Automated Biometric Identification System, and the International Criminal Police Organization's (INTERPOL) biometric holdings. The SOF web-based architecture provides the most comprehensive match/no match search results possible to the user.

Users can query the DOD authoritative database by using the SOF NIPRNET architecture located at <<http://id.socom.mil>>. After submission, the SOF user will receive an initial match report. Users can also submit the files over SIPRNET. After submission, the user will receive an initial match report and biometrics-enabled intelligence (BEI) support from USSOCOM'S BACC.

USSOCOM Biometric Analysis and Coordination Cell

USSOCOM's BACC provides support to the CJSOTF and NATO SOF teams by supplying near real-time, all-source intelligence to SOF exploitation submissions. The BACC provides BTIPs based on information derived from match reports, such as watch list matches, matches to latent prints from improvised explosive devices, or based on customer requests. BTIPs are provided as BEI for the teams to assist with targeting or as part of the prosecution packet.

After providing initial support, the BACC continues to develop BTIPs as follow-on analysis of high-valued individuals or in response to biometric matches to SOF exploitation submissions supporting strategic or national interests. The BACC also collaborates with the National Ground Intelligence Center sending matches for development of further intelligence and strategic analysis. The BTIPs and other products are distributed to the appropriate units or agencies. All products are loaded for search by the Distributed Common Ground Systems—Army, Intelink, and the Combined Information Data Network Exchange System, making them available for broad usage. The result is that USSOCOM's biometric efforts in Afghanistan are shared globally.

SOF Biometric Equipment

SOF are equipped with Cross Match® SEEK and Cogent® Fusion. Both devices provide durable, lightweight, multimodal, live biometrics collection. Users can also extract files from the Biometric Automated Toolset or any other device that produces a compliant file and submit those files to the USSOCOM portal.

Over the past four years, SOF and SOF associates operating in Afghanistan and around the world have successfully submitted 127,696 biometric files that resulted in 42,481 positive identifications, of which 1,674 were watch listed individuals. SOF operating in Afghanistan are able to collect biometrics and receive detain/release decision data within 15 minutes. SOF-collected biometric files and associated BEI are archived on the SOF exploitation website and available to anyone with SIPRNET access. BACC-produced BEI is shared with tactical, operational, and strategic assets and stored for continuing availability and use.

Appendix G

Center for Army Lessons Learned Lesson of the Day: Kandahar Biometric Data Collection

MAJ Larry Gnewuch, CALL Theater Observation
Detachment Officer

Dated: 22 July 2010

1. Observation: Biometric collection is making unprecedented improvements in security and governance across Kandahar City and the province. On 6 June 2010, a biometric enrollment center was stood up at the governor's palace. Afghans are biometrically enrolling the local populace and handing out biometric enrollment cards at a rate of 450 individuals per day. The Afghan enrollers are predominantly Kandahar University students in their mid 20s who feel they are doing something for their people by helping to take away the anonymity of the insurgents. They are being paid by Regional Command–South, through an incentive program fund for this noble effort to protect their city. This effort to have Afghans enroll Afghans directly supports the commander, International Security Assistance Forces (COMISAF) counterinsurgency (COIN) strategy to “build their capacity to secure their own country ... foster ownership ... and put them in the lead and support them, even before they think they are ready.” (*COMISAF COIN Strategy*, November 2009)

2. Discussion: Biometrics is the most effective nonlethal weapon system at controlling freedom of movement. It has been said that if we are able to secure Kandahar, the rest of the country will follow. That is why collecting biometric data from the population is so important in the battle to secure Kandahar City and the rest of the Kandahar province from the insurgents. Fifteen thousand local nationals have been enrolled at the governor's palace since June, with a goal of 50,000 enrollees by the end of August.

3. Observations, Insights, and Lessons: One of the lessons learned at the governor's palace enrollment station is that the Afghan enrollers are gathering full name, tribe affiliation, Tashkira number (most commonly used identity document in Afghanistan), and district they work in along with the biometric data. The standard for biometric collection in Afghanistan is to collect data on 10 fingerprints, two irises, and one facial picture. Task Force Biometric's support element in Kandahar employs a technique in which they set a unit Handheld Interagency Identity Detection Equipment to screen only the iris data against the biometric enabled watch list. It normally takes on average only 8–15 seconds to screen an iris against the watch list. Irises have proven to be 97 percent or better at positively identifying a person on the watch list during screening. On the other hand, it normally

takes two to three minutes to screen each fingerprint against the watch list (upwards of 20–25 minutes). Unlike iris screening accuracy, fingerprints have proven to be only 40–60 percent accurate. In essence, Soldiers will quite often receive possible matches while screening fingerprints, thinking they have matched against a person on the watch list, only to discover they have received a “false positive” when verifying the match against further data interrogation. Therefore, the lesson learned in screening only the iris data against the watch list is that it saves time (15–30 seconds for screening process versus 20–25 minutes) and it is much more accurate in analyzing the data and receiving a positive identification.

4. Recommendation: Continue with the innovative ideas being implemented at the governor’s palace in Kandahar City. Also, it is recommended that all combat outposts and checkpoints throughout Afghanistan make it a priority to collect biometric data from as many local nationals as possible. We need to create a sense of urgency with biometric collection. The sooner we are able to input the entire population of Afghanistan into the system, the sooner we will be able to match the 60,000 individual fingerprints lifted off improvised explosive devices and eliminate these insurgents from the battlefield. Biometrics is one of the biggest combat multipliers in the war in Afghanistan. If commanders treat it as such, the insurgents will no longer be able to hide among the local populace, and we will be one step closer to putting an end to this war.

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, the Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL website. The CALL website is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

<<http://call.army.mil>>

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL home page: "RFI or a CALL Product" or "Contact CALL."

**PROVIDE OBSERVATIONS, INSIGHTS, AND LESSONS (OIL) OR
SUBMIT AN AFTER ACTION REVIEW (AAR)**

If your unit has identified lessons learned or OIL or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

NIPR e-mail address: call.rfimanager@conus.army.mil

SIPR e-mail address: call.rfiagent@conus.army.smil.mil

Mailing Address:

**Center for Army Lessons Learned
ATTN: OCC, 10 Meade Ave., Bldg. 50
Fort Leavenworth, KS 66027-1350**

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at: <<http://call.army.mil>>. Use the "RFI or a CALL Product" link. Please fill in all the information, including your unit name and official military address. Please include building number and street for military posts.

PRODUCTS AVAILABLE “ONLINE”

CENTER FOR ARMY LESSONS LEARNED

Access and download information from CALL’s website. CALL also offers Web-based access to the CALL Archives. The CALL home page address is:

<<http://call.army.mil>>

CALL produces the following publications on a variety of subjects:

- **Combat Training Center Bulletins, Newsletters, and Trends**
- **Special Editions**
- ***News From the Front***
- **Training Techniques**
- **Handbooks**
- **Initial Impressions Reports**

You may request these publications by using the “RFI or a CALL Product” link on the CALL home page.

**COMBINED ARMS CENTER (CAC)
Additional Publications and Resources**

The CAC home page address is:

<<http://usacac.army.mil/cac2/index.asp>>

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <<http://usacac.army.mil/cac2/cal/index.asp>>.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history. Find CSI products at <<http://usacac.army.mil/cac2/csi/csipubs.asp>>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <<http://www.usapa.army.mil>> or the Reimer Digital Library <<http://www.adtdl.army.mil>>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <<http://fmso.leavenworth.army.mil/>>.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <<http://usacac.army.mil/cac2/militaryreview/index.asp>>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA Threats at <<https://desint-threats.leavenworth.army.mil/default.aspx>> (requires AKO password and ID).

Combined Arms Center-Capability Development Integration Directorate (CAC-CDID)

CAC-CDIC is responsible for executing the capability development for a number of CAC proponent areas, such as Information Operations, Electronic Warfare, and Computer Network Operations, among others. CAC-CDID also teaches the Functional Area 30 (Information Operations) qualification course. Find CAC-CDID at <<http://usacac.army.mil/cac2/cdid/index.asp>>.

U.S. Army and Marine Corps Counterinsurgency (COIN) Center

The U.S. Army and Marine Corps COIN Center acts as an advocate and integrator for COIN programs throughout the combined, joint, and interagency arena. Find the U.S. Army/U.S. Marine Corps COIN Center at: <<http://usacac.army.mil/cac2/coin/index.asp>>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <<https://jcisfa.jcs.mil/Public/Index.aspx>>.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

Center for Army Lessons Learned 10 Meade Avenue, Building 50 Fort Leavenworth, KS 66027-1350

Celebrating 25 years of uninterrupted support to the warfighter



Commander's Guide to Biometrics in Afghanistan



**US Army
Combined
Arms Center**

"Intellectual Center of the Army"

www.leavenworth.army.mil

U.S. UNCLASSIFIED//FOR OFFICIAL USE ONLY
REL NATO, GCTF, ISAF, ABCA
EXEMPT FROM MANDATORY DISCLOSURE under FOIA Exemptions 2 and 5