CONCEPT OF OPERATIONS FOR BIOMETRICS IN THE US CENTRAL COMMAND AOR

Version 2.0

March 2007

Table of Contents

1. (U) Purpose
2. (U) Applicability
3. (U) Responsibilities
3.1. (U) USCENTCOM
3.2. (U) USCENTCOM subordinate units
4. (U) The joint operational environment
5. (U) The USCENTCOM Joint Biometrics Process
5.1. (U) Overview
5.2. (U) Collection
5.3. (U) Process
5.4. (U) Analyze
5.5. (U) Decide
5.6. (U) Act
5.7. (U) Feedback
6. (U) Joint expeditionary employment of biometrics (use cases)
6.1. (U) Overview
6.2. (U) Biometrics support to offensive operations.
6.2.1.(U) Targeting
6.2.2.(U) Forensics captures
6.2.3.(U) Tactical questioning
6.2.4.(U) Population screening
6.3. (U) Biometrics support to force protection
6.3.1.(U) Access screening operations
6.3.2.(U) Entry control points (ECPs)
6.4. (U//FOUO) Biometrically enabled intelligence support to Operations
6.4.1.(U) Post operation analysis (BDA)
6.4.2.(U) Effects
6.4.3.(U//FOUO) Interrogation
6.4.4.(U//FOUO) Targeting
6.4.5.(U) Pattern and link analysis
6.4.6.(U//FOUO) HUMINT. See Annex E
6.4.7.(U//FOUO) Intelligence specific standards
6.4.8.(U) NGIC support
6.5. (U) Detention operations
6.5.1.(U) Detainee operations
6.5.2.(U) Track detainees inside a facility
6.6. (U) Civil-Military Operations (CMO)
6.6.1.(U) Manage local populations
6.6.2.(U) Track payments to foreign individuals
6.6.3.(U) Medical aid
6.6.4.(U) Prohibitions
6.7. (U) Information assurance

6.8. (U) Access management
6.9. (U) Personnel recovery
6.10. (U) Datasets/watch lists
6.11. (U) Other datasets
6.12. (U) Sharing of datasets
7. (U) Systems support requirements to biometrics
7.1. (U) Overview
7.2. (U) Fingerprints
7.3. (U) Processing of fingerprints
7.4. (U) Non-Fingerprint databases
7.5. (U) Irises
7.6. (U) DNA
7.7. (U) Speaker recognition
7.8. (U) Hand geometry
7.9. (U) Palm prints
7.10. (U) Facial photos
7.11. (U) Analysis
8. (U) Systems employment
8.1 (U) Authorized systems
8.2. (U) Approved systems as a constraint on Commanders
8.3. (U) Types of biometric captures
9. (U) Constraints and policies
9.1. (U) Overview
9.2. (U) Biometric capture constraints
9.3. (U) Biometric sharing constraints
9.4. (U) Situational exceptions
9.5. (U) Commander's exceptions

Annex A- (U) System crosswalk
Annex B- (U) Terms and glossary
Annex C- (U) References and policies
Annex D- (U) Collection standards and mandatory collection fields
Annex E- (S//NF) HUMINT Biometrics Management

1. (U) Purpose. This Concept of Operations (CONOP) documents concepts and procedures for the use of biometric technologies to support identity superiority, protection and management in the entire USCENTCOM AOR. This CONOP focuses on the biometrics process and key systemic enablers. This CONOP contains UNCLASSIFIED and CLASSIFIED annexes. The body of the CONOP is UNCLASSIFIED however, Annex E, "HUMINT Biometrics Management", is CLASSIFIED SECRET//NOFORN.

2. (U) Applicability

2.1. (U) This CONOP applies to all USCENTCOM components, CJTFs and subordinate commands within the USCENTCOM AOR, whether or not that collection occurs on or off of a U.S. controlled installation, including naval operations conducted in the offshore areas assigned to Commander, USCENTCOM.

2.2. (U) This CONOP also applies to other U.S. Government agencies operating biometric devices within the USCENTCOM AOR, if any of the following conditions exist:

- If such use is on any U.S. or coalition controlled installation.
- If the biometric device is in the AOR and will exchange data with any USCENTCOM biometric system.
- If the biometric collection operation will utilize any USCENTCOM personnel or communications system for its operation.

3. (U) Responsibilities

3.1. (U) USCENTCOM

3.1.1 (U) The Deputy Director for Operations is the General Officer (J3) with overall responsibility for Biometrics at USCENTCOM and works in close consultation with the Director of Intelligence (J2) and the Director of Command, Control, Communications, and Computer Systems (J6) and the Resources and Assessment Directorate (J8).

3.1.2. (U) The USCENTCOM Biometrics Advisory Board (CBAB) is the central coordination and decision point for biometrics doctrine, training, employment and fielding of supporting biometric technologies within the USCENTCOM AOR.

It consists of representatives from J3, J2, J6, and J8 and other Directorates as required.

3.1.3. (U) J3-JSO and J2-O jointly support biometrics actions in support of the CBAB. J3-JSO is the CBAB proponent for Force Protection related mission sets while CCJ2-O is the CBAB proponent for intelligence related mission sets.

3.1.4 (U) The Joint Information Management Board (JIMB) is responsible for building the CJTF information management plan. They identify and validate information exchange requirements and provide these to the C6. JIMB must approve all changes made to the theater network.

3.1.5. (U) All USCENTCOM organizations must send biometric requirements to J3-JSO, via chain of command, for actions.

3.1.6. (U) USCENTCOM's CBAB will serve as the official AOR interaction with DoD agencies, PM Biometrics, INSCOM, JFCOM and the DoD Principle Staff Advisory for all theater level requirements.

3.1.7. (U) CCJ3-JSO will consolidate USCENTCOM biometrics requirements for presentation to the JROC and Joint Staff for action.

3.2. (U) USCENTCOM subordinate units:

3.2.1. (U) All USCENTCOM subordinate organizations will receive USCENTCOM approval for the use of new biometric collection, processing, or storage systems prior to entry and use in the USCENTCOM AOR. This will help ensure overall compatibility with current supporting infrastructure and overall biometric enterprise.

3.2.2 (U) All USCENTCOM subordinates will establish a single staff section as the command proponent for biometric issues and functions.

3.2.3. (U) All USCENTCOM subordinate organizations will abide by the standards in this document.

3.2.4. (U) All USCENTCOM subordinate organizations will coordinate additional biometric requirements through USCENTCOM J3.

3.2.5 (U) All USCENTCOM subordinate organizations will produce a biometric CONOP. At a minimum, subordinate organization CONOPs will include all use case scenarios listed in this CONOP as well as the infrastructure required to support them.

3.2.6. (U) USCENTCOM subordinate organizations will send biometric requirements to J3-JSO for action.

4. (U) The Joint Operational Environment

4.1 (U) Biometrics is a key enabler across the entire range of military operations (ROMO) from credentialing US Persons on a network to Non-Combatant Evacuation Operations (NEO) to matching a latent print to a detainee. When used properly, it can lead to decisive results.

4.2 (U) Central to this environment is the categories of individuals. For the purposes of biometrics, an individual will fall into one of three categories: Red, Blue or Gray. An individual may transition from blue or gray to red as more information is collected, or move in the other direction. A "Red" individual is considered a clear threat to USCENTCOM interests while a "Blue" identity poses no threat. The third category, "Gray" is an individual whose motives are not clear and require future adjudication.

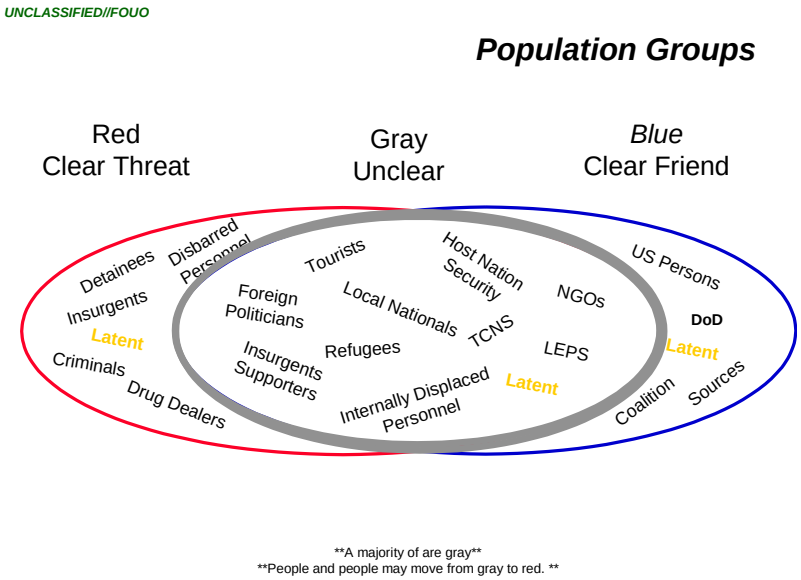


Figure 1: Categories of Individuals

4.3 (U) Biometrics is means of identification that provides great confidence in the relationship between an identity and an individual. The associated history of a biometric identity can assist in the categorization of individuals as "Red," "Blue," or "Gray." When properly collected and matched, biometrics routinely identifies an individual with a degree of certainty of over 99%. Unlike signatures or "flash to pass" ID cards, biometric samples cannot easily be faked. Unlike simple facial photos that change over time, a biometric proves more stable over time and cannot be easily duped through disguising.

4.4 (U) Biometrics is a force multiplier. By linking an individual to a history, a Commander has facts on which to base a decision. Biometric modalities provide faster screening while ensuring threatening personnel are identified. Because an individual's biometric modalities are not easily "spoofed" or transferable to another individual, a biometrics reader in lieu of a 'flash to pass' badge system is required. This type of verification allows the Commander to focus his forces on missions rather than determining the authenticity of credentials.

4.5. (U) Biometrics is also the only form of identification which, by its nature, is also evidence. By properly enrolling a person, a Commander can compare the match to

previously collected data such as latent prints, previous detainments, and 'watch lists.' A Commander can match an enrollment for base access or weapon card applicant against a historical latent print and use that history to deny access, and prosecute suspect individuals. Alternatively, biometrics systems can be used to exonerate innocent individuals by establishing irrefutable evidence of time/location combinations that can be accessed after the fact.

5. (U) THE USCENTCOM Joint Biometrics Process

5.1. (U) The purpose of the USCENTCOM biometrics process is to enable the Commander to effectively categorize an individual as friend or adversary. With biometrics, the Commander can match an individual to historical data in order to confirm that person is who they claim to be and possibly determine past activity.

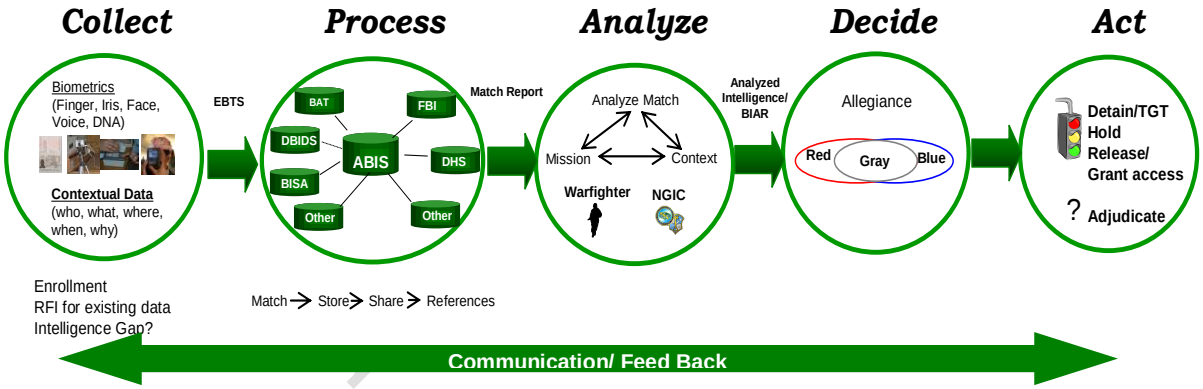


Figure 2: The USCENTCOM Biometrics Operational Process

5.2.(U) Step one is collection. It is the capture of the specific biometric modalities and contextual data based on the use case scenario. For biometrics capture, trained operators are preferred to ensure collection to DoD and USCENTCOM standards. Poorly collected biometrics cannot be matched and will create a false sense of security.

5.2.1. (U) The USCENTCOM standard for capturing biometric samples is based on the task. Enrollment, identification or verification require different captures. In all cases, capturing all the required biometric samples to standard is

key in order to maintain an effective database. Annex D contains a technical description of these requirements.

5.2.2. (U) When collecting biometrics, proper collection of contextual data is as important as proper collection of the biometrics. Contextual data not only establishes a contextual baseline for the individual, but it also drives exploitation and analysis. For example, it could establish aliases for an individual which can be used in support of both tactical questioning and interrogation.

5.2.3. (U) Enrollments will be as complete and accurate as possible. USCENTCOM biometric data is shared with DoD data collected in other theaters, the Department of Homeland Security (DHS), the Federal Bureau of Investigations (FBI), and other government agencies, as well as other governments. Simply putting a person on "Alert" or on a watch list with no associated contextual data marginally supports decision making. Thorough, complete contextual data will enable operations.

5.2.4. (U) Proper enrollment enables tracking of individuals. People move both between locations and migrate between "Blue" "Gray" and "Red" populations. A person may be enrolled as a police officer one day and match a latent print in the future. Another person may have been truthful in his first enrollment and lied in his second enrollment. If that is properly noted in the contextual data, it will drive tactical questioning and interrogation in the future.

5.2.5. (U) After enrollment, USCENTCOM uses verification by a credential (badge) to track individuals. If badges are not feasible, then identification using an existing database will be conducted. See paragraph 7 and Annex A for discussion of each.

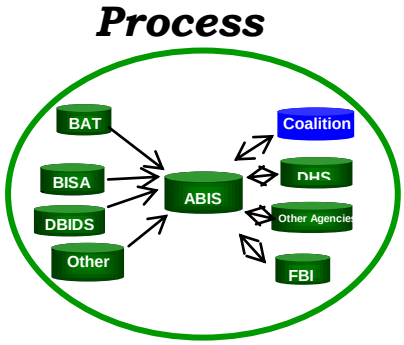


Figure 2.1: The USCENTCOM Biometrics Operational Process

5.3. (U) Step two is the processing of the data. It begins when the biometric data is matched to existing biometrics in the authoritative database and ends when it is made available to consumers to reference. The authoritative database has the capability to send information to other biometric databases across the US Government and with foreign friends and allies. When the authoritative database is not available, a local trusted database can be used for an interim match.

5.3.1. (U) A potential match is only as good as the data it is matched against. If a Commander decides to match off an incomplete (local trusted) database, he will not match against all available records and risk either not detaining a person of interest or detaining someone who should have been identified as friendly.

5.3.2. (U) Once biometrics are submitted to the ABIS, they are stored at the authoritative database. This data is then immediately available for other users to match against and may be shared as required for future use. For instance, reports can be generated to show the historical pattern of an individual accessing a base which may assist in the adjudication process if the individual requests to access other bases.

5.3.3. (U) Processing of the data is complete when all references have been searched and a 'dossier' of historical instances and associated contextual data is produced. It can be as simple as a 'match report' that resembles a

police 'rap sheet' or as complex as a 'digital dossier' containing multiple instances of the individual, full Screening Interrogation Reports (SIRs), HUMINT reports or other information.

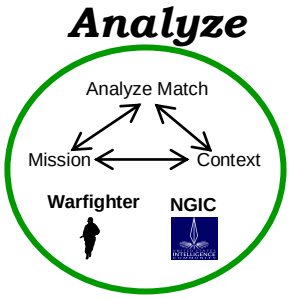


Figure 2.2: The USCENTCOM Biometrics Operational Process

5.4. (U) Once processing is complete, the results are analyzed. Simply knowing an individual matches another enrollment is of minimal value. Analysis drives tactical questioning and interrogation enabling the Commander to make the best decision possible. This can be as simple as a Navy Seaman comparing a match report in context to an Expanded Maritime Interdiction Operations (EMIO) operation or as complex as the National Ground Intelligence Center (NGIC) producing a Biometric Identification Analysis Report (BIAR) from a latent fingerprint match.

5.4.1. (U) The match report is generally sufficient to tactically question but not detain an individual of interest. The match report is very timely and effective means for driving questioning. However, simply because an individual was matched to a previous enrollment is not necessarily a logical link between the two events. For example, because an individual has been denied access to a given facility or area does not necessarily make him a threat. Similarly, a latent fingerprint that matches a base access applicant only associates that individual with an object. He may have touched the object at any time for a variety of reasons. However, an individual who applies for base access and matches to a latent fingerprint could present a threat.

5.4.1.1. (U) The match report is also the basis for biometrically enabled all source analysis in support of operations. These are used forward in intelligence cells

along with all other INTs in support of targeting, effects and interrogations. They are also used as part of joint evidence cells in support of prosecution.

5.4.2. (U) The NGIC produced BIAR is a processed intelligence product which associates a match to the circumstances. It is produced by analyzing the match, the individual's history, and all sources of intelligence.

5.4.2.1 (U) A BIAR is produced for all latent matches and other high value matches. Commanders may request BIARs directly from NGIC for other matches.

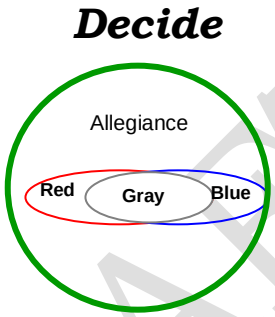


Figure 2.3: The USCENTCOM Biometrics Operational Process

5.5. (U) Analysis provides recommendations to the Commander, which aid in decision making. Based on the analysis the Commander will decide whether the individual is a threat (red), a friend (blue) or undetermined (gray). Categorizing persons in this manner helps Commanders quickly provide enough information to the US military member to make a decision and act on the information provided.

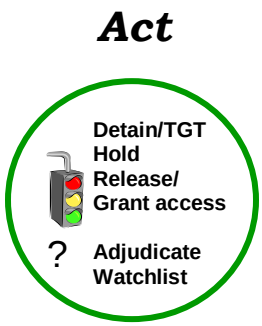


Figure 2.4: The USCENTCOM Biometrics Operational Process

5.6. (U) Once the Commander has decided whether the individual is a threat, he acts. Actions taken toward an individual determined to be a threat will vary upon constraints. If an individual is determined by the Commander to be a threat (red), that individual is generally detained for prosecution or targeted. All latent print matches will be treated as hostile until a BIAR is produced and/or the circumstances adjudicated. If an individual is detained or awaiting access to base and is subsequently confirmed to be friendly (blue), the decision is usually to release him or grant him base access.

5.6.1. (U) A key decision is what to do with an individual that remains unknown (gray) after biometrics matching and exploitation. The Commander may decide there is further adjudication needed. Simply because there is no biometric match does not mean a person is blue or red. Commanders must consider the context of a match (or lack thereof) when adjudicating the disposition of an individual.

5.7. (U) Feedback is critical throughout the process. At each step of the process Commanders must assess the quality and timeliness of the information to ensure it supports their decision making. Also, when an action is taken such as "release from detention", Commanders must notify all persons and organizations that require feedback to maintain an accurate database.

6. (U//FOUO) Joint Expeditionary Employment of Biometrics (Use Cases).

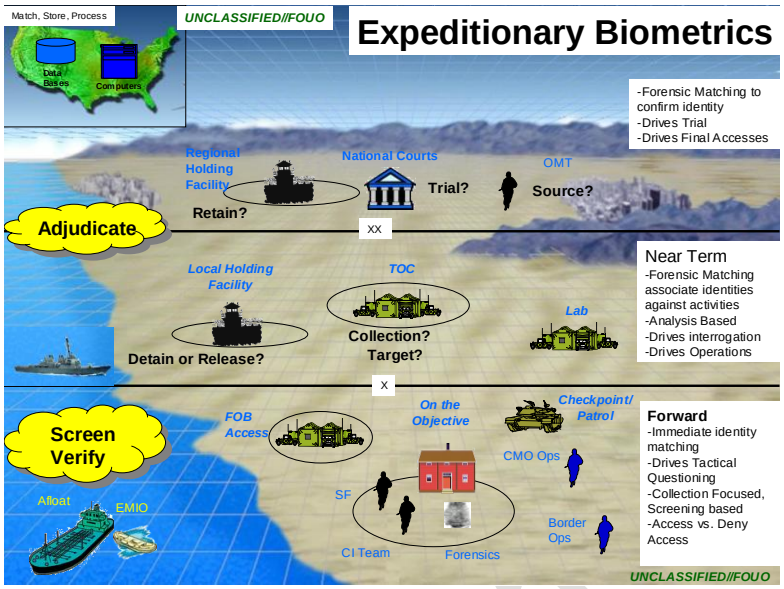


Figure 3: The USCENTCOM Biometrics Employment

6.1. (U) Biometrics enables the full range of military operations in the USCENTCOM AOR. The process is driven by the Commander's decisions. Commanders may use biometrics to screen populations based on histories, verify individuals or decide access based on biometrically-enabled adjudication.

6.1.1. (U) Annex A contains the time standards and products associated with each of the mission sets below.

6.2. (U) Biometrics Support to Offensive Operations.

6.2.1. (U) Targeting. Just as with a photo, biometrics are used in support of targeting an individual. By pre-loading information on a targeted individual or group of individuals, Commanders can create a tailored, biometrically enabled, target set.

6.2.2. (U) Forensics Captures. Latent fingerprints link targeted individuals with events. Biometrics may confirm an individual was present at an event with a high degree of certainty. They are also suitable to assist in long term detainment and prosecutions of individuals.

6.2.3. (U) Tactical questioning. Biometrics matching on the objective may confirm an individual's identity and allow the appropriate authority to make a decision

concerning that individual, for instance either hold or release. Using the associated contextual data and the history of that individual within the context of the encounter may provide service members enough information to tactically question a person and separate targets from bystanders.

6.2.4. (U) Population Screening. Biometrics can be used to segregate populations based on several factors. For example, at a check point a Commander may use biometrics to determine if a person is out of place or has been previously granted access. Marines use biometrics (iris matching) to determine if a person at a checkpoint is a resident of the city or not. If the person is not, they are segregated, enrolled and further questioned.

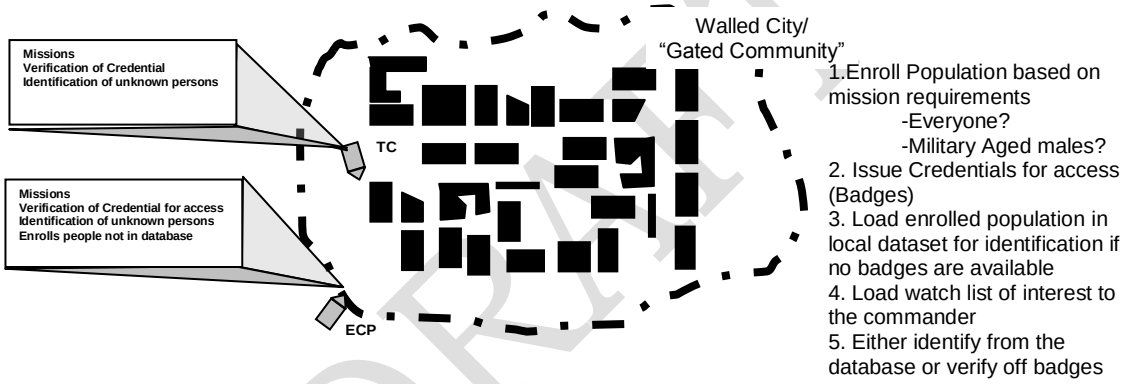


Figure 3.1: Biometrics Support to Population Screening

6.3. (U) Biometrics Support to Force Protection.

6.3.1. (U) Access Screening Operations. Units using biometrics can determine if a person is who he or she claims to be, denying their ability to hide under an alias or remain anonymous. Biometrics and the associated contextual information enable the unit to determine an individual's history to a high degree of certainty for use in adjudication of base access requests.

6.3.2. (U) Entry Control Points (ECPs). Individuals are verified at ECPs prior to being granted access to bases. Instead of 'flash to pass' ID badges that can be easily faked and must be manually scanned, a biometric can quickly confirm an identity, increasing accuracy and saving time and manpower.

6.3.2.1. (U) USCENTCOM uses biometrics for individuals that do not have a credential. If they are confirmed in the database, they are allowed access IAW unit TTPs. If not, they may be enrolled for further adjudication.

6.4. (U//FOUO) Biometrically Enabled Intelligence Support to Operations

6.4.1. (U) Post Operation Analysis. A Commander, using biometrics, can assess the impact of given individual to his or her area of responsibility. Individuals found to be historically blue may provide a sense of comfort while if a red individual is identified that threat may be reduced.

6.4.2. (U) Effects. USCENTCOM uses biometrics to assess the effectiveness of a mission. Using a biometric, you can confirm the identity of a targeted person post operations. With biometrics, you can confirm with a high degree of certainty a unit has captured/killed the right individual.

6.4.3. (U//FOUO) Interrogation. Interrogators may confirm an individual is who he claims to be using biometric matching. They can also use biometrics to determine the history of an individual (previous accesses/detentions, previous aliases) to drive the interrogation plan. Using a dossier they can check previous interrogations to determine which methods were employed in previous detentions.

6.4.4. (U//FOUO) Targeting. Biometrics, as with photographs, must be part of all targeting folders if available. Targets with known biometrics will be loaded on watch lists. For those targets without biometrics, biometric collection will be requested through the RFI process and stated as an intelligence gap.

6.4.5. (U) Pattern and Link Analysis. Biometrics matching provides a means of relating events. Matching latent prints to other latent prints may associate attacks with an individual. These associations are used to conduct pattern analysis in support of predictive analysis and future targeting. Similarly, a biometrically-enabled history can highlight patterns of an individual who is known, was once believed to be "Blue," and has, through any number of mechanisms, been determined to be a threat. Pattern and

link analysis can also give rise to targeting – that is, if an individual has been biometrically encountered in the vicinity of numerous suspect events, that pattern might be sufficient for a tentative identification of the person as Red.

6.4.6. (U//FOUO) HUMINT. See Annex E for discussion of biometrics in support of HUMINT operations.

6.4.7. (U//FOUO) USCENTCOM standard for intelligence support is enrollment and identification. Hasty enrollment will not be used for this mission. When ever an individual is encountered, he will be checked. If he is not in the database, he will be enrolled.

6.4.8. (U) NGIC provides USCENTCOM all source analysis based on biometric matches through BIARs. BIARs may be posted on NGIC's AIMS portal and/or emailed to organizational and individual email accounts of the unit that captured the biometric.

6.4.9. (U) If a biometric is not available, it will be stated as an intelligence gap. There are non-DoD collected biometrics available. If an individual was arrested by another nation and applied for another country's credentials, or was the subject of national-technical collection, there may be a biometric available for comparison.

6.5. (U) Detention Operations

6.5.1. (U) Detainee Operations. USCENTCOM uses biometrics to ensure the right person is, or remains, detained or released with a high degree of certainty. Biometrics confirm a known identity to an individual detainee and his associated contextual data, which may include current location and reason for detention.

6.5.2. (U) Track detainees inside a facility. Biometric are used to track detainees. While in transit, USCENTCOM uses biometrics to establish their location. While in the detainment facility, they are used to track movement within the detainment facility and track location.

6.5.3. Prosecution. Biometrics support prosecution of detainees. Using biometrics, a Commander can match an enrollment for a detainee to a latent match and use that in prosecution of a case. Using other analytical tools, a Commander can associate the object the latent came from (for example, a sniper rifle) with other historical events. Beyond a latent, a Commander can use biometrics to establish an individual's previous detentions to establish patterns of misconduct.

6.6. (U) Civil-Military Operations.

6.6.1. (U) Manage Populations. USCENTCOM uses biometrics to manage local populations during military operations. From tracking non-combatants during a NEO to managing an Internally Displaced Persons (IDP) camp, USCENTCOM uses biometrics to track which individuals are authorized a service or access to a location with a high degree of certainty. Using biometrics, a Commander can accurately state how many people he has in a camp or has evacuated without risking double counting.

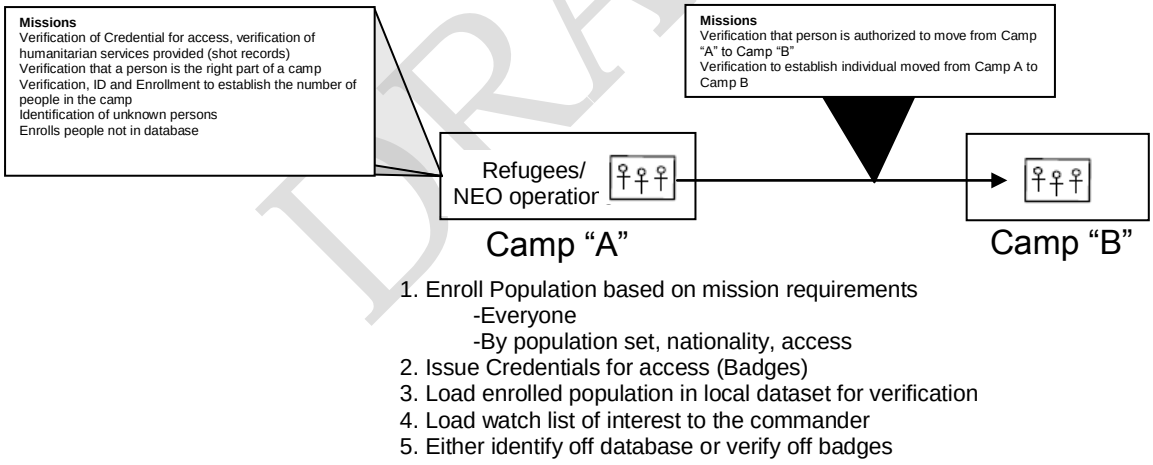


Figure 3.2: Biometrics Support to NEO/Refugee Operations

6.6.2. (U) Track Payments. USCENTCOM uses biometrics to track payments to foreign individuals. Using biometrics, a Commander can track which contractors were paid. Using the associated contextual data, a Commander can ascertain what was paid and for what actions. The key to this is that biometrics last beyond a transition of authority (TOA) and can exist across units.

6.6.3. (U) Medical aid. USCENTCOM uses biometrics to track medical aid. Commanders are authorized to enroll individuals to track medical assistance or procedures (shots, etc…) are given to an identity or to verify the identity at a later date.

6.6.3.1. (U) Biometrics captured exclusively as a result of medical treatment will be shared and sent to the ABIS IAW with medical data sharing constraints. However, biometrics captured as result of force protection operations in support of the medical treatment (i.e., if the clinic is on base or 'inside the wire') will be sent to the ABIS.

6.6.4. (U) Under no circumstance will units assigned to USCENTCOM deny humanitarian services solely because an individual refuses to provide a biometric. However, biometrics will be captured for force protection reasons.

6.7. (U) Information Assurance.

6.7.1. (U) Information Assurance. USCENTCOM uses biometrics to conclusively verify the identity of those attempting to gain access to information systems. On networks, a biometric token can be used to confirm an individual identity and his or her permissions, similar to base access.

6.8. Access Management.

6.8.1. (U) Access Management. Outside of combat operations, USCENTOM authorizes biometrics for access management. For example, as persons depart a ship they can be biometrically verified to establish who has left the ship. As they embark they can be verified again to establish with a high degree of certainty the number of individuals, and which individuals, are onboard the ship.

6.9. Personnel Recovery.

6.9.1. (U) Personnel Recovery. USCENTCOM uses biometrics during personnel recovery operations to verify individuals. For example, a unit may conduct a mission to retrieve a kidnapped individual. The unit could frontload the data on a man portable system, which can then be used to verify the identity of the individual of interest.

692
693
694
695

6.10. (U) Datasets/Watch lists.

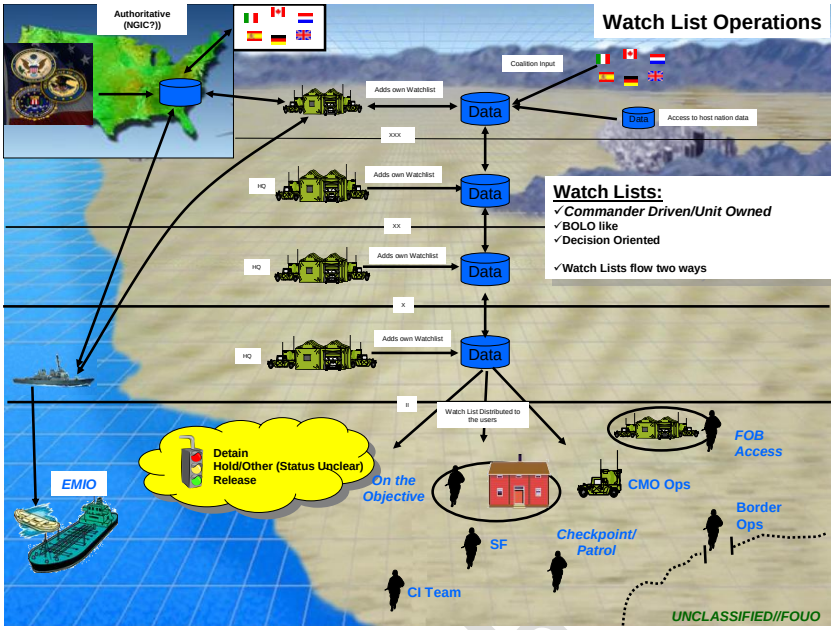


Figure 4: The USCENTCOM Watch list Process

6.10.1 (U) Watch list. Watch lists are datasets of individuals of interest to a Commander. They are individuals the Commands want their units to act on, based on the encounter. The action may be detain, release or hold for further exploitation.

6.10.2. (U) Watch list datasets are generated and shared at every level of command (fig 4.). They are driven by individual unit requirements and command decisions. Commanders can direct their datasets of interest and select additional data from adjacent units, higher HQ or consolidate all subordinate units.

6.10.3. (U) These datasets are a key enabler for stand alone (untethered) operations. Often times, Commanders will find that their units cannot reach the authoritative or even a local trusted database. In this case, the watch list becomes a tool the service member can quickly check against and take action upon.

6.10.4. (U) These datasets speed (or decrease) match times. Instead of checking *1:All* the data is check *1:Some*. This can decrease match times on the objective, or at an ECP, by a factor of ten.

6.10.5. (U) Finally, these datasets enable Commanders to share their individuals of interest. A Commander may have a local leader in his sphere of influence whom the Commander wishes to track but not detain. That individual's biometric can be shared and added to the watch list as "Do not detain." A suspected bomb maker could be flagged as a 'hold' based on the circumstance of the encounter. Finally, a Commander may want to target an individual. That individual's record can be flagged as 'detain' for the next encounter.

6.11. (U) Other Datasets

6.11.1. (U) Other Datasets. Beyond watch lists, USCENTCOM uses local trusted datasets ("skeleton" databases/local databases) to decrease match times and increase throughputs. A Commander can decide to locally retain a portion of the database for command use. For example, while conducting population management a Commander may have a local database containing only persons authorized access to an area to enable 'red light/green light' operations.

6.11.2. (U) Local trusted datasets will be used for verification and identification only. All new enrollments will be sent to the ABIS for matching and storage.

6.12. (U) Sharing of datasets

6.12.1. (U) Sharing. Datasets will also be created and shared with coalition partners in accordance with constraints outlined in paragraph 9 of this CONOP. These datasets will generally be the biometrics themselves along with unclassified contextual data.

7. (U) Systems Support Requirements to Biometrics

7.1. (U) USCENTCOM employs a biometrics joint enterprise system approach to biometrics to eliminate redundancy of effort. The hub of this system for fingerprints is the DoD Automated Biometrics Identification System (ABIS). Unless specifically noted in this CONOP, all data captured in the USCENTCOM AOR will go to the ABIS for matching and storage, regardless if a local trusted database is used.

7.1.1. (U) USCENTCOM is responsible for integrating all approved biometric systems into its architecture. USCENTCOM will approve any new system, or modification to existing system, to ensure interoperability with its architecture. This includes any biometric collected to any standard by all USCENTCOM components in the AOR.

7.1.2. (U) For non-DoD agencies operating in the USCENTCOM AOR, all data collected on a DoD facility or as part of a USCENTCOM mission will be integrated in the architecture.

7.1.3. (U) USCENTCOM fully supports all non-DoD agency interaction and interoperability with its architecture and will share its databases as required.

7.1.4. (U) USCENTCOM units employ biometrics collection and processing systems as either networked or stand alone systems. A networked systems match provides an authoritative match against ABIS or a local trusted database, while stand alone devices use a dataset ('watch list' or 'skeleton database') for local matching. However, all enrollment data and unmatched identification data, even if it is stand alone, will be sent to the ABIS for storage.

7.1.5.(U) Regardless of collection systems, USCENTCOM units will send all biometric fingerprint, face and iris data to the ABIS for storage and reference. Palm print data, when taken, must also be sent to the ABIS.

7.1.6. (U) The biometric priority order for collection is fingerprints, iris images and facial photographs. Components will collect DNA from detainees at the theater facilities along with palm prints. Components are authorized to collect to hand geometry and voice.

7.2. (U) Fingerprints.

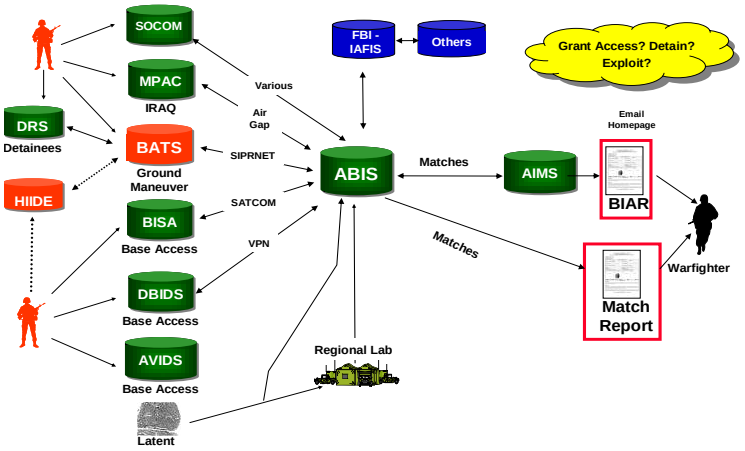


Figure 5: The USCENTCOM Biometrics Systems of Systems

7.2.1. (U) Fingerprints are captured IAW Annex D of this document.

7.2.2. (U) Collection of the biometric contextual data will be IAW Electronic Biometric Transmission Standard (EBTS) along with additional USCENTCOM-directed contextual data. A typical EBTS file is 700k-1.3 megabytes. See Annex D for all collection standards.

7.2.3. (U) If a live scan is not available, ink and paper will be used to capture fingerprints. If live scan and ink and paper are not available, capacitance sensors will be used provided they meet the standards in paragraph 7.2.2 and Annex D.

7.3. (U) Processing (Storage/Matching/Referencing)

7.3.1. (U) Outside of Biometrics Identification System for Access (BISA), all biometrics are initially processed and stored in local trusted databases. This allows local matches of some of the records but does not provide for matching against all available records.

7.3.2. (U) After matching against the local database, EBTS files will be sent to the ABIS for authoritative matching.

They are matched against all existing DoD records and stored for future matching. Networked systems will send their records to the ABIS within 6 hours of capture. Stand alone systems that capture new data on various missions must connect to a network as soon as practical after the mission is completed. Disconnected systems will send their records to the ABIS within 6 hours of reconnecting to the network.

7.3.3. (U) The ABIS is unclassified. Records sent to the ABIS via SIPRNET must be downgraded according to unit SOP. Ideally, new biometrics systems in the AOR will be 'born unclassified' allowing flexibility to be employed on any network. Biometric Automated Toolkit (BAT) records will be downgraded by NGIC.

7.4. Other Databases

7.4.1. (U) In addition to fingerprints, the ABIS contains iris and facial images. However, ABIS is not currently able to match based on those two modalities. Until these functionalities are achieved, local non-fingerprint matching databases will be used. There are series of trusted databases: for face and iris, BAT databases accomplish this role. Units requiring a match from the BAT database must merge the files into BAT as an EBTS. For DNA, there is no authoritative DoD database; however, matches can be conducted *one to one* to verify a known individual from the Armed Forces DNA Identification Laboratory (AFDIL) database.

7.5. (U) Irises

7.5.1. (U) Both irises images will be captured as part of all enrollments. Annex D contains a technical description of the requirement.

7.5.2. (U) Irises can be used for all biometric missions and are a fast, non-intrusive means of verifying and identifying persons to a high degree of certainty. Identification of individuals using irises on a man-portable system can be conducted in less than 3 minutes.

7.5.3. (U) Units can use a BAT enrollment station, HIIDE or Pier 2.3 to verify identity.

7.5.4. (U) All systems capturing irises images will send their data to ABIS for storage.

7.5.5. (U) Until the ABIS is capable of matching iris images, all matches will occur on local BAT databases and there will be no BIAR produced. Units may request a BIAR on iris matches through NGIC.

7.6. (U) DNA

7.6.1 (U) DNA will be collected on all detainees when they are moved into the TIFs using Buccal Swabs (Q-Tip on the inside of the person's cheek).

7.6.2. (U) DNA will be forwarded to the Armed Forces DNA Identification Laboratory (AFDIL) for processing and retention.

7.6.3. (U) DNA matches will be sent to NGIC for intelligence analysis and a possible BIAR

7.6.4. (U) Annex D contains a technical description of DNA capture requirements.

7.6.5. (U) DNA collected as a part of a forensic investigation can be locally stored and processed.

7.7. (U) Speaker Recognition

7.7.1. (U) Speaker recognition is the matching of an individual identity to a voice.

7.7.2. (U) There are no current ANSI/NIST standards for speaker recognition nor processors/databases for matching, however USCENTCOM recognizes the RAPTR ACDT (CHAMPION) as the short term future tool set in development for this standard.

7.7.3. (U) USCENTCOM does not endorse the capturing of voice without a standard. However, units may capture voice data based on mission needs.

7.8. (U) Hand Geometry

7.8.1. (U) Hand geometry is not required biometric enrollment unless it is specifically required for local verification missions.

7.8.2. (U) Hand geometry is authorized for verification only. It will not be used for identification.

7.8.3. (U) Hand geometry data will not be sent to the ABIS.

7.9. (U) Palm Prints

7.9.1. (U) Palm prints are not required for all enrollments.

7.9.2. (U) Effective 90 days after the release of this CONOP, palm prints must be taken from detainees and mailed to the ABIS for matching. Effective 30 days after this CONOP is released all detainees must have their palm prints captured. Screening against the ABIS will be conducted as capability is available.

7.9.3. (U) Palm prints capture will include the palm area and the 'writer's palm'- the area on the outside of the palm between the pinky and the wrist. The image will be 1,000 ppi.

7.9.4. (U) Annex D contains a technical description of the requirement.

7.10. (U) Facial Photos

7.10.1. (U) 5 facial photos will be taken as part of all enrollments. Annex D contains a technical description of the requirement.

7.10.2. (U) With the exception of detainees in Guantanamo, facial photos will be UNCLASSIFIED and sent to the ABIS for matching and storage.

7.10.3. (U) Photos of detainees in Guantanamo will be handled IAW paragraph 9 of this document and DepSecDef memo dated June 2, 2006.

7.11. (U) Analysis

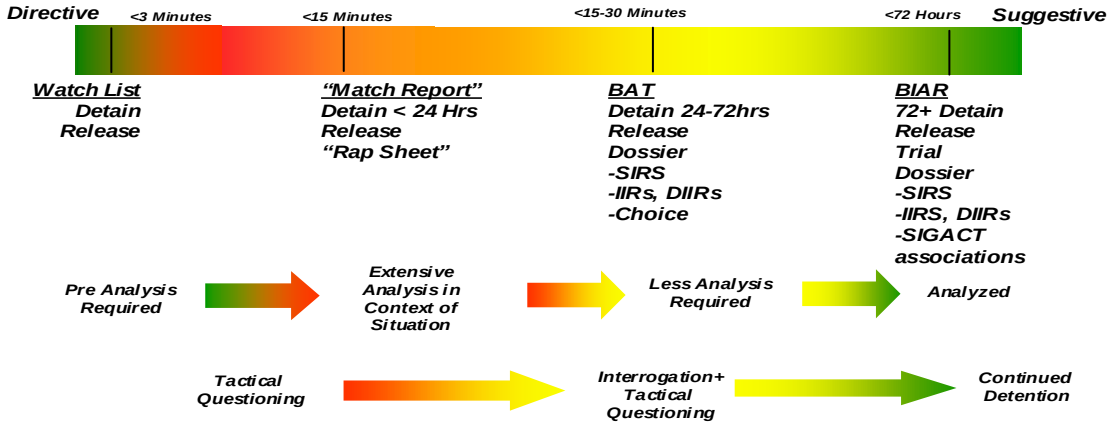


Figure 6: Analysis

7.11.1 (U) Once a biometric match is made, it must be analyzed based on the previous instances of the individual and the associated contextual information. This can be done forward based on a BAT-generated match report or through NGIC's BIAR portal (AIMS) or the Marines Joint Prosecutorial Exploitation Center (JPEC).

7.11.2. (U) The match report is an ABIS report or BAT dossier. These reports cover a known history of instances of encounters of an individual. These match reports will list the previous encounters of the individual but not provide analytical amplification. For example, a match report for a person mistakenly detained and then released after 48 hours will look very similar to a person detained for 14 days but released for lack of evidence. On the other hand, a latent matched to an IED discovery may be because the person discovered the IED and contaminated the

evidence. Match reports are well suited for tactical questioning and development of an interrogation plan.

7.11.3. (U) The BIAR is less timely but more in depth. Standard processing time is less than 6 hours (for a certain subset of matches), though it can be accelerated upon request. Unlike a match report, BIARs are processed analytical products that associate the individual with his or her known history and include more than just the biometric. BIARs are usually sufficient to support long term detention or to support adjudication of a person's status. For example, in a case of an IED latent match, NGIC will go back to the SIGACT (significant activity) and determine if the latent was the result of incidental contact with the IED. They will also evaluate the location of the latent to provide feedback to help determine if the person was involved in the assembly or emplacement.

8. (U) Systems Employment

8.1 (U) Figure 7 shows biometrics systems that are approved to enable missions in the USCENTCOM AOR. The green boxes (filled in) are the USCENTCOM-recommended and supported systems for the selected missions. Of note, BISA is the approved base access solution for Iraq and DBIDS for the remainder of the AOR. The SOCOM Special Operations Identity Dominance (SOID) kit, for identification and enrollment, is approved for all SOCOM mission sets.

8.1.1. (U) Additional system uses or upgrades must be approved by the USCENTCOM Biometrics Advisory Board (CBAB) prior to employment. Contact CCJ3- Biometrics for further information.

8.1.2. (U) As part of the CBAB approval process, all new systems will be tested by the Biometrics Fusion Center (BFC) for technical interoperability, compliancy, and data capabilities prior to submission for approval. The BFC will test to ensure they meet DoD and USCENTCOM standards and are in accordance with USCENTCOM Regulation 25200 for impacts to the network.

	Tactical Missions							
Operational System	Targeting/Maneuver	Force Protection	Intelligence Operations	Detainee Operations	CMO	IA	Access Management	Coalition
BAT	✓	✓	✓	✓	✓			✓
EMIO Tool Set	✓				✓			✓
BISA	✓	✓			✓		✓	
DBIDS	✓	✓					✓	
MPAC								✓
HIIDE	✓				✓			
DRS				✓				
AVIDS								
ESE	✓							
SOID	✓				✓			✓

Figure 7: The USCENTCOM Approved Systems
Green is the recommended system

8.2. (U) Commanders should not assume this diagram is a constraint on any operations and may employ their systems based on mission needs. However in doing so they accept the risk that using an improper biometric tool will not meet their requirements.

8.3. (U) Types of Capture

8.3.1. USCENTCOM recognizes three types of biometrics capture- enrollment, identification and verification. See Annex A figure 1-1 and 1-2 for a crosswalk of mission types to biometrics encounters.

8.3.2. (U) The USCENTCOM standard for an initial or suspected initial encounter of an individual is enrollment. The USCENTCOM standard for follow-on encounters of the individual is verification. When there is doubt about whether an individual has been previously enrolled and there is time, USCENTCOM Commanders are directed to conduct full enrollments.

8.3.2.1. (U) Enrollment is the creation of a biometric record for the purpose of retaining this file in the DoD authoritative database. It will be stored for future matching and be shared with other national and international agencies.

8.3.2.1.1. (U) USCENTCOM expects 'full enrollment' for all detainee operations, access privileges, and in any situation where time allows for full enrollment.

8.3.2.2. (U) USCENTCOM enrollment consists of rolled fingerprints, 5 facial photos, both irises and contextual data. DNA and palm prints are also required for detainee enrollments.

8.3.3. (U) Identification is the establishment of an identity through matching against an existing enrollment. It can be off an existing dataset (watch list), local trusted database (BAT) or trusted or authoritative source including a secure credential.

8.3.3.1. (U) The USCENTCOM standard for identification is matching an enrolled record against one of the following: both thumbs and both index fingers, a four finger slap print, or both irises. These techniques generally produce high confidence in the match result. Total planning time for identification is 3 minutes in a communications-rich environment, 30 minutes in an austere environment.

8.3.3.2. (U) All biometrics captured but not matched as a part of an identification will be sent to the ABIS for storage and possible matching. If commanders have reason to believe that an individual may not otherwise be enrolled, they will conduct a full enrollment as circumstances allow.

8.3.4. (U) Verification is the matching of an individual to an existing biometric *1:1*. It usually involves matching a credential (a base or area access card) to an individual. There is no new information captured and it is merely a comparison to an existing capture.

8.3.4.1. (U) Because verification does not involve the capture of a biometric nor the inclusion of any of the contextual data, it can be conducted using a capacitance reader.

8.3.4.2. (U) Verification data can be used to collect historical information on individuals, but under no circumstances will the data be used as a substitute for an enrollment or identification. If an individual fails to verify data, that individual will be enrolled.

8.3.5. (U) Hasty enrollment is anything less than a full enrollment. Though the goal is full enrollment, USCENTCOM realizes that based on mission needs Commanders may not have the time to conduct a full enrollment.

8.3.5.1. (U) Hasty enrollments are not suitable for complete processing and thorough analysis. Due to the potential of decreased quality and quantity of biometrics captured from hasty enrollment, they may have minimal value for future matching, and they limit the ability to match against data from other US agencies and governments.

8.3.5.2. (U) Commanders are authorized to conduct a hasty enrollment as an exception only, provided they accept the risk of incomplete data checks and chance of 'false negative' results. Commanders will capture as much data as possible but must accept these risks. For example, if a Commander elects to only capture 4 prints, he is missing 60% of possible latent matches. If a Commander uses less than a full finger scanning device, he will only be able to match off less than 7% of latent prints. In addition to restricting the ability to match against existing records, hasty enrollments decrease the reliability of future match attempts against the individual who is not being fully enrolled, and against matching with other US Government agencies.

8.3.5.3. (U) If the subject requires adjudication based on the hasty enrollment (detention, accesses, etc…) a full enrollment must be conducted.

8.3.5.4. (U) Biometrics captured as result of a hasty enrollment will be sent to the ABIS for storage and possible matching.

8.3.5.5. (U) Biometrics captured as result of hasty enrollment is incomplete and the ABIS cannot generally share it with the FBI, other agencies, or foreign governments. Given that the FBI only accepts full enrollments, biometrics captured in hasty enrollments will not be as useful for homeland security or global counter-terrorism.

9. (U) Constraints and Policies

9.1. (U) Foreign and domestic laws, policies, regulations, and cultural inhibitions may limit, prohibit or restrict the employment of biometrics capabilities. For example, the Privacy Act forbids the sharing of US Persons' (Citizens and US Resident Aliens) biometric data without their knowledge. Also, European Union member nations have more stringent restrictions on sharing biometrics.

9.2. (U) Biometric Capture Constraints

9.2.1. (U) With the exception of US Persons and Coalition Government/ Military members, current DoD policy directs the capture of biometrics on all personnel voluntarily desiring access to US Bases, facilities and installations in the USCENTCOM AOR.

9.2.2. (U) Commanders can, as part of a criminal investigation, capture US Persons' biometrics if they are suspected of terrorist or criminal acts without a signed privacy act. Generally, collection of biometrics for criminal acts by US Persons on US installations, bases or FOBs will not be sent to the ABIS for matching.

9.2.3. (U) Commanders can make biometric enrollment a condition of employment or voluntary access to DoD facilities in the USCENTCOM AOR regardless of nationality. If so, a privacy act must be signed.

9.2.4. (U) Personnel with dual US citizenship are considered US Persons for purposes of biometrics collection.

9.2.5. (U) Personnel whose citizenship is uncertain are considered non-US Persons and not coalition government/ military members for purposes of biometrics collection.

9.2.6. (U) Commanders can capture biometrics of deceased or wounded individuals. With the exception of known US Persons, Commanders will use their discretion in determining if the deceased will be treated as "Red, Gray or Blue."

9.2.7. (U//FOUO) HUMINT data collection will be handled IAW Annex E to this document.

9.2.8. (U) Biometrics captured exclusively to track medical support will be clearly marked in that individuals record to prevent unintentional release of their data.

9.2.9. (U) Biometrics captured exclusively as part of a NEO operation will be clearly marked with the mission name and individual's country of origin to prevent unintentional release of the data.

9.2.10. (U//FOUO) Facial photos of detainees in Guantanamo will be treated as classified IAW DepSecDef memo dated June 2, 2006.

9.3 (U) Sharing constraints.

9.3.1. (U) Classification. Unless specifically noted, the biometric itself will be treated as Sensitive but Unclassified (SBU).

9.3.2. (U) Commanders will not share US Persons' biometrics with non-US government organizations without a privacy act statement specifically authorizing such sharing. Privacy Act statements must include the organization(s) the data will or can be shared with. This includes the biometric itself (image, template or minutia) and its associated contextual information.

9.3.2.1 (U//FOUO) Commanders can request exceptions to paragraph 9.3.2 through the CBAB for Known Suspected Terrorist US Persons only.

9.3.3. (U) Commanders will not share coalition members' biometric data without approval from USCENTCOM. This includes the biometric itself (image, template or minutia) and its associated contextual information.

9.3.4. (U) Commanders will ensure that all US Person and EU members are appropriately identified in the associated contextual data.

9.3.5. (U) Classified biometrics and/or associated contextual data will be shared as applicable though FDO channels.

9.3.6. (U) Commanders will share all other biometrics with approval from USCENTCOM CBAB.

9.3.7 (U) Personnel with dual citizenship are considered US Persons for purposes of biometrics sharing.

9.3.8. ((U//FOUO)) Data collected through HUMINT channels will not be shared without approval of USCENTCOM CCJ2-X.

9.3.9. (U) Biometrics collected exclusively to track medical support will shared IAW medical information release polices.

9.3.10. (U//FOUO) Facial photos of detainees in Guantanamo will not be shared without approval of the unit's FDO and USCENTCOM CCJ3.

9.4. (U) For circumstances not covered in paragraph 9.1-9.2, Commanders will use their judgment, to include consideration of and, when applicable, abiding by host nations laws and customs when collecting biometrics.

9.5. (U) Nothing in paragraphs 9.1-9.3 prohibits the Commander from, in exceptional circumstances, conducting biometric enrollments of a population set or sharing biometrics to protect the force from an immediate threat.

9.6. (U) Under no circumstance will units assigned to USCENTCOM deny humanitarian services solely because an individual refuses to provide a biometric. However, biometrics will be captured for force protection reasons.

Annex A- System Crosswalk

	Mission	Network	Mission	Modality	Time	Product -
RED FORCE Database	**Offensive Operations -**	SIPRNET, untethered	Identification	2x Index Finger and 2x Thumbs or 2 x Iris, XX key fields	Off watchlist, < 3 minutes, Off other <15 Minutes	Red Light/Green Light orMatch Report/Rap Sheet
			Enrollment	10x rolled, 2x Slaps, 2x Iris, 5x Facial Photos, All Fields	<15 Minutes against ABIS and local DB	History of encounters, RAP sheet
	Force Protection	NIPRNET, SIPRNET, untethered	Verfication	Hand Geometry, 1 x Index finger of credential	<30 Sec off credential (badge)	Red Light/Green Light
			Identification	1x Index Finger w/ credential, 2x Index Finger and 2x Thumbs or 2 x Iris without	<3 Minutes against local DB, <24hrs from ABIS	Red Light/Green Light orMatch Report/Rap Sheet
			Enrollment	10x rolled, 2x Slaps, 2x Iris, 5x Facial Photos, All Fields	<30 minutes to enroll, answer w/i 24 hours	BIAR
	Intelligence Operations	SIPRNET, tethered	Identification	10x rolled, 2x Slaps, 2x Iris, 5x Facial Photos, All Fields	<15 Minutes	BIAR, RAP Sheet
	Detainee Operations -	SIPRNET, tethered	Identification	2x Index Finger and 2x Thumbs or 2 x Iris	<30 Minutes against local DB, <24 Hrs from ABIS	Red Light/Green Light orMatch Report/Rap Sheet
			Enrollment	10x rolled, 2x Slaps, 2x Iris, 5x Facial Photos, All Fields	<30 minutes to enroll, answer <24 Hrs hours from ABIS	BIAR
RED or Blue force Database	**CMO**	NIPRNET, SIPRNET, untethered	Verfication	1x Index Finger w/ credential	<30 Sec off credential (badge)	Red Light/Green Light
			Identification	2x Index Finger and 2x Thumbs or 2 x Iris, XX key fields	<3 Minutes against local DB, <24hrs from ABIS	Red Light/Green Light or Match Report/Rap Sheet
			Enrollment	10x rolled, 2x Slaps, 2x Iris, 1x Facial Photo, CMO fields	<30 minutes to enroll, answer w/i 24 hours	BIAR
Blue Force	**Information Assurance**	NIPRNET, SIPRNET	Verfication	1x Index Finger (US Person)	<15 Sec off credential (CAC Card)	Red Light/Green Light
			Identification	1x Index Finger (US Person)	<3 Minutes against local DB, <24hrs from DEERS/RAPID	None
			Enrollment	1x Index Finger (US Person)	<10 minutes to enroll,	None
	Access Management	NIPRNET, SIPRNET, untethered	Verfication	1x Index Finger off CAC card	<10 Sec off credential (CAC Card)	Red Light/Green Light
			Identification	1x Index Finger from DMDC database	<3 Minutes against local DB, <24hrs from DEERS/RAPID	Complete History of previous encounters establishing identy and encounters
	Personnel Recovery	NIPRNET, SIPRNET, untethered	Verfication	1x Right Index finger off CAC card	<10 Sec off credential (CAC Card)	Confirmation of Idenity (Green Light)
			Identification	2x Index Finger and 2x Thumbs against DMDC database or DNA from AFDIL database	<3 Minutes against local DB, <24hrs from DEERS/RAPID	Complete History of previous encounters establishing identy and encounters

Figure 1 to Annex A
Mission Cross walk

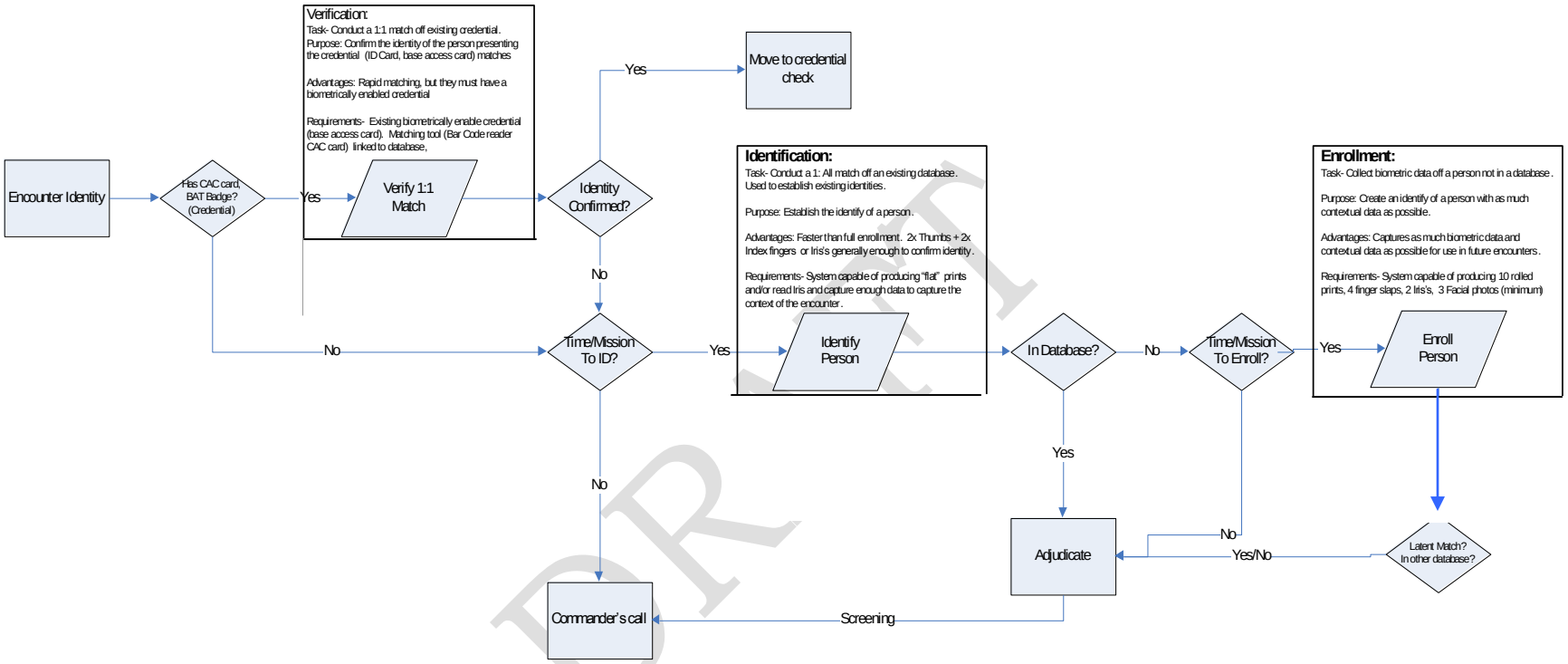


Figure 2 to Annex A
Mission Flow Chart

Annex B
Glossary AND Terms

Terms

1:1
A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one) and the identification task can be accomplished by a series of one-to-one comparisons.

Adjudication
To determine an individual's status or accesses.

Attempt
The submission of a single set of biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual.

Analyze/Analysis
To examine critically to determine the elements or bring out the essence of an identity. For example, comparing a match in context of the encounter to determine allegiance, or to evaluate a history of encounters to determine intent.

Authoritative Database
The single verified database which contains data entities referenced by all other databases. In a tiered approach, it is the highest level database.

Badge
A distinctive card bearing identifying information, usually name, and affiliations (unit, agency) and credentials. See credentials.

Biometrics
A general term used alternatively to describe a characteristic or a process.
As a characteristic:
A measurable, unique or distinguishing biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition.
As a process:
Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric Data
A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations.

Biometric System
Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of:
1. Capturing a biometric sample from an end user
2. Extracting and processing the biometric data from that sample
3. Storing the extracted information in a database
4. Comparing the biometric data with data contained in one or more reference references
5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved.

A biometric system may be a component of a larger system.

Capacitance Sensor
A sensor which employs the ratio of compressed charge a conductor to determine the biometric. Generally, a live scan device (see live scan).

Capture
The process of collecting a biometric sample from an individual via a sensor for submission. See Submission.

Characterization of an identity/Individual
Determination of an identity as known friend (blue), known enemy (red) or unknown (gray).

Collection
The process of capturing biometric samples, distinguishing characteristics, background and associated contextual data in order to identify or enroll an individual.

Comparison
Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision.

Credential
Evidence of authority, access or rights or privileges. With biometrics, it can be in the form of a badge or digitally on a chip or database. *(The PKI chip on the CAC card contains a credential)*

D-Prime (D')
The process of determining an individual's status or access.

Database
A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related end user information, etc.

Decision
The characterization of the individual based on the biometric match and adjudication, which leads to the determination of what action will be taken.

Disbarment List
A list of people denied base access. See watch list and credential.

End User
The individual who will interact with the system to enroll, to verify, or to identify.

Enrollment
The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Enterprise
A common venture. For biometrics, a common set of systems and processes used to achieve identity dominance.

Face Recognition
A biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

Feature(s)
Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference.

Fingerprint Recognition
A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important

features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings.

Hamming Distance
The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity.

Hand Geometry Recognition
A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

Hasty Enrollment
An incomplete enrollment not generally suitable for matching all available modalities.

Identification
A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database.

Identity
Unchanging physical and personal characteristics of an individual. Who a person is regardless of alias's or previous personas.

Indifferent User
An individual who knows his/her biometric sample is being collected and does not attempt to help or hinder the collection of the sample. For example, an individual, aware that a camera is being used for face recognition, looks in the general direction of the sensor, neither avoiding nor directly looking at it. *See*

Intelligence
The result of analysis by a trained analyst.

Interim Match
A match by a database other than the ABIS prior to matching the ABIS.

Iris Recognition
A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes, as illustrated below. The iris muscle is the colored portion of the eye surrounding the pupil.

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

Live Capture
Typically refers to a fingerprint capture device 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).

Local Trusted Database
A database, other than the ABIS, which is validated by the Commander for local matching.

Match
A decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity

Matching
The process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold.

Mimic
The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter.

Modality
A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

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.

Non-cooperative User
An individual who is not aware that his/her biometric sample is being collected. Example: A traveler passing through a security line at an airport is unaware that a camera is capturing his/her face image.

Palm Print Recognition

A biometric modality that uses the physical structure of an individual's palm print for recognition purposes, as illustrated below.

Pixels Per Inch (PPI)
A measure of the resolution of a digital image. The higher the PPI, the more information is included in the image, and the larger the file size.

Platen Size
The size of the sensor plate used collect a finger or palm print. For example, the FBI standard for rolled prints is a 1x1 platen.

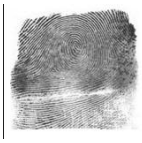
Population
The set of potential end users for an application.

Recognition
A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply the verification or identification (watch list).

Record
The template and other information about the end user (e.g. name, access permissions).

Reference
The biometric data stored for an individual for use in future recognition. A reference can be one or more templates, models or raw images.

Rolled Fingerprints
An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor, as illustrated to the left.



Segmentation
The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression, as illustrated below.

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

Silent Match
A match from a database where the distribution of the match and/or associated contextual data is limited to small group or agency based "on need to know." Normally, it is reserved for classified information or classified mission.

Silent Notification
A match from a database where notification is either limited to small group or agency based "on need to know" or an agency is notified outside of normal processing. Normally, it is reserved for classified information or classified mission.

Slap Fingerprint
Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card, as illustrated to the left. Slaps are known as four finger simultaneous plain impressions.

Speaker Recognition
A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said, and is not a biometric technology.

Spoof/Spoofing
The ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database.

Submission
The process whereby an end user provides a biometric sample to a biometric system in order to verify, enroll or identify.

Template

A digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison.

Throughput Rate
The number of biometric transactions that a biometric system processes within a stated time interval.

Uncooperative User
An individual who actively tries to deny the capture of his/her biometric data. Example: A detainee mutilates his/her finger upon capture to prevent the recognition of his/her identity via fingerprint.

Verification
A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.

Vet/Vetting
The process of determining an individual's allegiance, background or suitability for credentialing. See adjudication and decision.

Watch list
A list of identities of interest to a Commander, unit or organization.

Acronyms

ABIS = Automated Biometrics Identification System
AFDIL = Armed Forces DNA Identification Lab
AIMS = Automated IDENT Management Support
ANSI = American National Standards Institute
AOR = Area of Responsibility
AROC = Army Requirements Oversight Council
BAC = Biometric Analytic Cell
BAT = Biometrics Automated Toolset
BEI = Biometric Enable Intelligence
BFC = Biometrics Fusion Center
BIAR = Biometrics Intelligence Analysis Report
BISA = Biometrics Identification System for Access
BIR = Biometric Intelligence Repository
BTF = Biometrics Task Force
CBAB = CENTCOM Biometric Advisory Board
CBT = Computer Based Training
CEXC = Combined Explosives eXploitation Cell
CITP = Counter-IED Targeting Program
CJIS = Criminal Justice Information Services Division (FBI)
COCOM = Combatant Command
CONOP = Concept of Operations
CONUS = Continental Untied States
COPS = Centralized Operation Police Suite
DBIDS = Defense Biometric Identification System
DCGS-A = Distributed Common Ground System – Army
DHS = Department of Homeland Security
DNA = Deoxyribonucleic Acid
DMDC = Defense Manpower Data Center
DMS = Detainee Management System
DoD = Department of Defense
DOJ = Department of Justice
DOS = Department of State
DRS = Detainee Reporting System (NDRC / OPMG)
EBTS = Electronic Biometrics Transmission Specification
EFTS = Electronic Fingerprint Transmission Specification
EIS = Enterprise Information Systems (PEO)
EMIO = Expanded Maritime Interdiction Operations
FBI = Federal Bureau of Investigation
FSE = Field Support Engineer
HOA = Horn of Africa
HIIDE = Handheld Interagency Identity Detection Equipment
HVT = High Value Target

IAFIS = Integrated Automated Fingerprint Identification System
IBOS = Intelligence Battlefield Ops System
IEDD TF = Improvised Explosive Devices Defeat Task Force
IEW&S = Intelligence, Electronic Warfare and Sensors (PEO)
IIR = Intelligence Information Report
JAB = Joint Automatic Booking Station (FBI version of BAT)
JFAADD = Joint Federal Agencies Antiterrorism DNA Database
JCIDS = Joint Capability Integration and Development System
JIOC-I = Joint Intelligence Operations Capability – Iraq
JPEC = Joint Procedural Exploitation Cell
JROC = Joint Requirements Oversight Council
JUONS = Joint Urgent Operational Needs Statement
LEAs = Law Enforcement Agencies
LEDET = US Navy, with a US Coast Guard Law Enforcement Detachment
LTO = Language and Technology Office (USAIC & FH)
MIO = Maritime Interdiction Operations
MNF-I = Multinational Forces Iraq
MPAC = Multi-Purpose Access Card
MSC = Major Subordinate Command
NDRC/S = National Detainee Records Center / System
NGIC = National Ground Intelligence Center
NII = Network and Information Intergation
NIPRNet = Non-secure Internet Protocol Router Network
NIST = National Institute of Standards and Technology
OASD = Office Assistant Sec Def
OEF = Operation Enduring Freedom
OIF = Operation Iraqi Freedom
ONS = Operational Needs Statement
OPMG = Office of the Provost Marshal General
PISCES = Personal Information Secure Comparison Evaluation System (DOS)
PEO = Program Executive Office
PDA = Personal Digital Assistant
PM / PMO = Program Manager / Program Management Office
POR = Program of Record Office
P&R = Personnel and Readiness
PSA = Principal Staff Assistant
SBU = Sensitive But Unclassified
SIGACT = Significant Activity

SIPRNet = Secret Internet Protocol Router Network
SOF = Special Operations Forces
SOID = Special Operations Identity Dominance
SOP = Standard Operating Procedures
TEDAC = Terrorist Explosive Device Analytical Center
THT = Tactical HUMINT Team
TIB/TIG = Theater Intelligence Brigade / Group
TRADOC = US Army Training and Doctrine Command
TSM = TRADOC Systems Manager
TTP = Techniques, Tactics and Procedures
UNS = Universal Needs Statement (USMC)
USAIC & FH = US Army Intelligence Center & Ft. Huachuca
WIT = Weapons Intelligence Team
XML = eXtensible Markup Language

Annex C
References and Policies

Policies are posted at:
http://hqswebj2.centcom.smil.mil/biometrics/policy /index.asp

1. (U) Deputy Secretary of Defense Memorandum, "Force protection Identity Screening for Base Access", (29 MAR 05).

2. (U) Electronic Fingerprint Transmission Specification (EFTS) Version 7.1 , (May 05), http://www.fbi.gov/filelink.html?file=/hq/cjisd/iafis/efts71/efts71.pdf.

3. (U) American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST)- ITL 1-2000, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information," (Sep 00), ftp://sequoyah.nist.gov/pub/nist internal reports/sp500-245-a16.pdf.

4. (U) "Products certified for compliance with the FBI's Integrated Automated Fingerprint Identification System image quality specifications," http://www.fbi.gov/hq/cjisd/iafis/cert.htm.

5. (U) ANSI/INCITS 385-2004, "Face Recognition Format for Data Interchange," (May 04). This standard is copyrighted and licensed copies are available from the DoD BMO.

6. (U) NIST Best Practice Recommendations for the Capture of Mugshots, Version 2.0, (Sep 97), http://www.itl.nist.gov/iad/vip/face/bpr mug3.html.

7. (U) Department of Defense Biometrics Management Office Website, http://www.biometrics.DOD.mil.

8. (U) FBI Procedure on Taking Legible Fingerprints, http://www.fbi.gov/hq/cjisd/takingfps.html.

9. (U) ANSI/INCITS 379-2004, "Iris Image Interchange Format," (May 04). This standard is copyrighted and licensed copies are available from the DoD BMO.

10. (U) DA Form 2663-R, "Fingerprint Card," http://www.apd.army.mil/pub/eforms/pdf/a2663_r.pdf.

11. (U) Assistant Secretary of Defense (Networks & Information Integration) Memorandum titled "Establishment of a DoD Automated Biometric Identification System (ABIS)," 05 Aug 04.

12. (U) DoD Electronic Biometric Transmission Specification (EBTS), Version 1.2, (08 Nov 06) http://www.biometrics.dod.mil/Documents/DoD_ABIS_EBTS.pdf

13. (U) HSPD-6 Integration and Use of Screening Information (September 16, 2003) (http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html).

14. (U) HSPD-11 Comprehensive Terrorist-Related Screening Procedures (http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html).

15. (U) HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors (http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html).

16. (U) Federal Information Processing Standard (FIPS) 201 (http://csrc.nist.gov/publications/fips/fips201/FIPS-201-032006.pdf).

17. (U) Executive Order 13356: Strengthening the Sharing of Terrorism Information to Protect America (August 27,2004) (http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html).

18. (U) OMB M-04-04: E-Authentication Guidance for Federal Agencies (http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf).

19. (U) OMB M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf).

20. (U) OMB M-03-22: OMB Guidance for Implementing the Privacy Provisions the E-Government Act of 2002 (http://www.whitehouse.gov/omb/memoranda/m03-22.html).

21. (U) DoD Directive 1000.25 "Personnel Identity Protection," July 19, 2004.

22. (U) Deputy Secretary of Defense Memorandum, "Executive Agent for the Department of Defense (DoD) Biometrics Project", 27 December 2000.

23. (U) DoD Standard Operating Procedure (SOP) for Collecting and Processing Detainee Biometric Data (11 FEB 05).

24. (U) Army Regulation 190-8, "Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees," (Oct 97), http://www.usapa.army.mil/pdffiles/r190_8.pdf.

25. (U) CFC FRAGO 09-596 [BIOMETRIC COLLECTION SYSTEM AND REPORTING SYSTEMS] dated 17 JUN 04.

26. (U) Annex G, MNF-I Access Control Policy, to MNF-I Memo 11-1, Command Policies and Procedures.

27. (U) DoD Policy for Biometric Information for Access to US Installations and Facilities in Iraq dated July 15, 2005.

28. (U) Message DTG 191903ZMAR07 "EMIO IDENTITY SCREENING CHANGE 1"

29. (U) DepSecDef on Classification of Photographs of Individuals Detained at Guantanamo dated June 2, 2006.

30. (U) DoD policy entitled "Sharing of Biometric Data and Associated Information from Non-U.S. Persons with Coalition Forces and Allies Date 10 January, 2006

31. (U) DoD policy entitled "Sharing of Biometric Data and Associated UNCLASSIFIED Information from Non-U.S. Persons with Interagency Entities date 10 January, 2006.

32. (U)

31. (U) Capstone Concept of Operations for DoD Biometrics Support of Identity Superiority date XX XXXX, 2006.

32. (U) Deputy Secretary of Defense Memorandum "Defense Biometrics" 4 October, 2006.

33. (U) Deputy Underscretary of the Army Memorandum "Executive Agent Status on Biometrics," 14 June, 2006.

34. (U) Joint Requirements Oversight Council (JROC) Memorandum "CENTCOM Short term Biometric Priorities," March 2007.

Annex D
Collection Standards and Mandatory Collection Fields

TBD