

MNF-W  
Biometric  
SOP



Version 1  
June 2007

## Table of Contents

### Commander's Guidance

#### Executive Summary

#### 1. Introduction

- A. Definitions
- B. Purpose
- C. Mission

#### 2. Guidance to Units

- A. Billets, Duties & Responsibilities
- B. Training
- C. Handling of Classified materials and Foreign Disclosure

#### 3. Operations

- A. Population Control
- B. Screening
- C. Enrolling
- D. Badging
- E. ISF Recruiting
- F. Detainee Procedures
- G. HVI, AIF Target Confirmation
- H. Base Access
- I. HIIDE Employment Considerations

#### 4. Information Management

- A. ALERT Status and Dossier Entry Management
- B. Watchlist Maintenance and Management

#### 5. Database Replication and Communications Networking

- A. Database Replication
- B. Communications Networking

#### 6. Equipment Supply, Maintenance, and Sustainment

- A. Supply
- B. Maintenance
- C. Sustainment

### Appendices

#### Part I

- A. Standards
- B. MNF Badge standards
- C. SOP for recording badges in BAT

## Part II

### **MNF-W Specific Training Techniques and Procedures (published separately)**

---

- A. Watch List Procedures and Maintenance**
  - B. Database Replication and Network Communications Procedures**
  - C. How to activate the BAT peripherals**
  - D. Identification and Enrollment Process**
  - E. How to correctly fill out the EFT during enrollment**
  - F. How to use Rapid Enrollment**
  - G. How to Upload Data to the Iris Device**
  - H. How to Link Entities (Vehicle Registration)**
  - I. How to Set up the BAT Badge Printer**
  - J. How to Record Resident Badges in BAT**
  - K. How to Export Copy data from Client to Server**
  - L. How to Set-up, Activate, and Upload Data to the HIIDE**
  - M. Definitions**
-

## Commander's Guidance.

---

As we continue our efforts to defeat AQI and neutralize the insurgency, the ability to employ biometric tools such as BAT (Biometric Automated Toolkit) provides us an operational advantage over AIF by denying them freedom of movement within the populace. Whether performing badging operations in Fallujah, Ramadi, or throughout AO Denver; executing immediate screening operations on potential detainees in the field; or screening potential Iraqi Security Forces (IP and IA); the effectiveness of the system is based on how well it is integrated across the spectrum of operations and how consistently we employ it.

It is critical that our Marines, soldiers and sailors who employ these systems understand the significance biometrics bring to the fight. As we expand the number of biometric systems across the AO, our ability to employ biometric tools to our advantage is dependent on two things: First, understanding and appreciating the tactical advantage biometrics brings (ability to identify both threat and friendly forces) and second; how consistently we integrate these tools with our tactics, techniques, and procedures. Biometrics is a force multiplier...use it.

Executive Summary.

Biometric Systems provide a critical capability in the counterinsurgency- that of positive identification of previously enrolled individuals. When employed correctly, they provide us the ability to deny enemy freedom of movement within the populace as well as identify known insurgents. Our primary biometrics system is BAT (biometric automated toolkit). BAT has many mission applications but in order to be effective, commanders must accomplish the following:

1. Designate an officer or SNCO to provide oversight at the battalion level to ensure biometric systems are effectively employed and integrated into unit operations.
2. Ensure adherence to basic procedures- such as how to scan badges or irises at an ECP. (For example it takes approximately **3 seconds** for the system to retrieve a file scanned by a bar code reader and confirm if an individual is on ALERT.)
3. Develop a plan to manage the information available in BAT. This includes establishing standards as to who can enter information and place people on ALERT and managing any unit WATCHLISTs employed in conjunction with the targeting cycle.
4. Develop a plan to keep each BAT system's database updated with the most recent information. (Accomplished by updating over the SIPRNET or by being manually updated by another system (aka the sneaker net).) Ideally, disconnected BAT clients are updated daily, but no less than weekly.
5. Develop accountability for all systems. BAT is a computer system with biometric peripheral devices. Enterprising Marines without the proper safeguards will adapt the system for other uses, despite the fact that it requires changing prohibited settings and is a CLASSIFIED system.
6. Evacuate broken systems through the normal maintenance chain for accountability to CLB where the ICE2 contractor takes them - ERO's should be opened and the gear will be exchanged 1:1 as available.
7. Ensure users understand what it means to be on ALERT vice just in the system. Records of individuals on ALERT are outlined in red. Individuals can be on ALERT for many reasons: Either the individual needs to be detained; or there is administrative information to be aware of. (For example, the ALERT text may read *DETAIN, USE CAUTION, UPDATE DATA, DO NOT RELEASE, DENIED ACCESS*).
8. Develop consistent employment practices which integrate into the unit's overall concept of operations.

MNF-W Standards.

*Throughout the SOP the MNF-W standards are listed in boxed text, and also collectively in SOP Appendix A.*

## 1. INTRODUCTION.

### 1. A. Definitions.

**ALERT List** is anyone in the BAT database that has been placed on alert and shows up in RED. Being on alert is distinguished from being on a WATCHLIST and can be administrative as well as to indicate an individual needs to be detained. There are less than 100,000 people on ALERT. WATCHLISTs are a subset of the ALERT list.

**Biometric Automated Toolset (BAT)** is an automated personnel enrollment and tracking system that collects biometric data. It incorporates iris scan, fingerprints, photo, and biographical information of an individual and stores the collected data onto a central server located on a secure network.

**Biometric file** is the individual data from an enrollment (biometric and textual data).

**Biometrics** is measurable physical and behavioral characteristics that establish and verify an individual's identity.

**BISA** is the Biometric Identification System for base Access is the system used by ATFP for local and third country national identification for base access.

**Contextual Data** are elements of biographical and situational information (who, what, when, where, how, why, etc.) that are associated with a collection event and permanently recorded as an integral component of a biometric file.

**Enrollment** is the process of capturing biometric data on an individual and entering it into the database. Required in order to badge. Never enroll US citizens unless they are a combatant.

**Field Support Engineers (FSE's)** are the primary contractors who support BAT and HIIDE. They are responsible for the network and database infrastructure as well as training maintenance and operational support to units. Other contractors include trainers, and potentially Biometric Systems Administrators (BSA) who are a combination of FSE and trainer at the unit level.

**Full Enrollment** consists using the BAT system to roll all ten fingers, two slaps of the four fingers on each hand followed by both thumbs, iris scan, photo scan, and full contextual data.

**HIIDE** is a portable, battery operated handheld multi-modal [iris, fingerprint, facial photo, biographic contextual information] biometric device that can support biometric identification and enrollment tasks.

**Rapid Enrollment** is an option on Version 4.0.4 version of BAT software. It has the ability to pre/auto-populate data fields and reduces processing time for enrolling. It also

can run concurrent operations of searches and enrollments, reducing overall processing time for groups.

**Screening** is the process of confirming whether a person is in the database or if a badge is valid and associated with an individual. BAT Badges provide for the fastest screening. The priority for screening in terms of speed and accuracy is the badge bar code or number (2-3 second retrieval of the individual's record), an iris scan against the ALERT LIST or WATCHLIST, (2-3 seconds to match) or screening an iris against the whole database (2-3 minutes if the system is operating correctly).

**WATCHLISTs** are the lists in the BAT database comprised by units or agencies of individuals to be detained if encountered. They can be loaded into HIIDE for screening or identity confirmation. The max total number of individuals on a WATCHLIST that can be loaded into a HIIDE is 10,000. Individuals on a WATCHLIST will always be on ALERT.

**1.B. Purpose.**

These Standard Operations Procedures (SOP) establish the MNF-W basic operating parameters for the employment of Biometrics systems focusing on the battalion and below employment of BAT (Biometric Automated Toolset) and HIIDE (Handheld Interagency Identification Detection Equipment) systems. This SOP establishes standards that all units will follow unless previously coordinated with MNF-W.

**1.C. Mission.** Biometric systems are employed to deny the enemy freedom of movement within the populace and positively identify known insurgents. They gather biometric data through incorporation of iris scan, fingerprints, photo, and contextual data.

Mission sets.

1. Population Control (screening, enrolling, and badging operations).
2. Screening and enrolling ISF.
3. Detainee procedures (local and RDF).
4. HVI and AIF Target confirmation (including KIA's).
5. Base access and local security.
6. HIIDE employment.

MNF-W will use BAT and HIIDE to identify AIF, friendly populace, LNs (Local Nationals), and TCNs (Third Country Nationals) throughout the AO to separate the insurgents and foreign fighters from the general population.

MNF-W will also employ BAT and HIIDE to positively identify high value individuals (HVI's), screen and badge Iraqi Security Forces (ISF), for force protection (e.g. local access) and for detention operations.

Having an effective BAT system requires integrating the operational, intelligence, and communications aspects of the program into a cohesive concept of employment. The standards for all three aspects are discussed in this SOP.

**2. Guidance to Units**

**2.A. Billets and Requirements.**

Units employing biometric systems (BAT, HIIDE, or BISA) will have a designated officer or SNCO who is responsible for ensuring the accountability, support, and employment of the system. For units employing BAT, the unit representative will ensure the following:

1. A specific plan is developed and adhered to for updating the database of all BAT clients. This includes client servers on the network and disconnected clients.
2. Ensure equipment and classified hard drives are accounted for appropriately.
3. Coordinate and ensure adequate training for operators to include staff representatives and S-2 personnel.
4. Develop expertise or subject matter experts in the areas of enrollment and screening, networking and database replication, database and WATCHLISTs management.
5. Develop limited training capability in lieu of FSE support.



For units employing HIIDE, the unit representative will ensure the update plan includes updating the WATCHLIST on each HIIDE as well as ensuring that the targeting cycle at the battalion or higher level incorporates a search of the BAT database for any possible HVI's to add to the watchlist.

MNF-W Standard for billets.

- *Units employing biometric systems will designate an officer or SNCO responsible for the overall employment of the system.*

**2.A (1) MNF-W Billets and Requirements.**

**MNF-W Information Management Officer (IMO).** The IMO maintains responsibility for integration, employment of biometric systems, and sustaining their utilization on the communications network architecture. He maintains OPCON of field support engineers (FSE's) and their employment in support of operations and the overall system and manages the MNF-W BAT portal site.

**MNF-W Intelligence Watch List Manager (G-2).** The G-2 Watchlist manager maintains overall responsibility for management of MNF-W Biometric WATCHLISTs and ensures the following:

1. Ensures current NGIC Biometric Intelligence Analysis Reports (BIAR) pertinent to MNF-W are promulgated through intelligence channels.
2. Ensures units maintain HIIDE/BAT WATCHLISTS with the most current target biometric files uploaded.
3. Coordinates with outside organizations (i.e. CEXC, WITT, CID etc) to ensure all latent unidentified biometric data pulled from crime scenes are placed on ALERT and added to biometric WATCHLISTS.
4. Accepts nominations from the MSC Watch list Managers for maintenance of the MNF-W and NGIC WATCHLISTs.
5. Ensures contact data and naming conventions in WATCHLISTs are adhered to and correct.

**Field Support Engineers and Representatives.**

**Field Support Engineer.** FSE's are the contract support that sustain the BAT system by maintaining the network architecture, replication, service and support to subordinate units, hardware troubleshooting and training. They are located in Camp Fallujah, Blue Diamond (Camp Ramadi) and Al Asad. Their priorities of effort for work follow:

1. Maintaining the network architecture that supports the overall biometric enterprise.
2. Maintaining network architecture and operational support at the battalion level.
3. Training operators on the employment of biometric systems.
4. Providing tactical support at the small unit level.

**MNF-W Database Manager.** The database manager performs a twofold function:

1. Ensures the accuracy of the data within the database from a network system standpoint (the completeness of files and overall health of the database from a software standpoint). This includes electronic maintenance of the database and WATCHLISTs.
2. Manages and facilitates access to the data in terms of searches, maintenance, and quality control of files as an aggregate.

**MNF-W Biometrics Trainer.** The MNF-W BAT/HIIDE trainer is a dedicated asset available to units to provide basic operator training, local networking (not on the tactical network) WATCHLIST training, and database employment training. MSC's coordinate requests and submit them to the MNF-W IMO.

## **2.A (2) MSC Billets and Requirements.**

**Biometric POC.** Units employing biometric systems will designate a representative responsible for integrating the operational, intelligence, and communications aspects of the program into a cohesive concept of employment.

**Requirements.** The associated requirements can be performed by one or more individuals.

1. Integration into operations and tactical employment of the system, including training.
2. Maintenance and management of biometric WATCHLISTs.
3. Replication of the BAT database as described in paragraph 5 and BAT SOP Part II, Appendix E.
4. Integration and sustainment on the tactical communications network, including system administration for clients on and off the tactical network.
5. Sustainment of the system for maintenance and consumables (such as for badging operations).

**Operators.** At the MSC level BAT uses designated, vice dedicated operators for intelligence analysis and targeting, as well as WATCHLIST management. This is performed on desktop clients and does not require operator enrollment and screening training.

Local security force and detention center operator employment fall under Battalion operations.

## **2.A (3) Battalion Billets and Requirements.**

**Biometric POC.** At the battalion level and below, BAT requires familiarization within the battalion staff for successful employment, establishment and adherence of standards, and updating the database. Battalions will designate a representative responsible for integrating the operational, intelligence, and communications aspects of the program into a cohesive concept of employment.

**Requirements.** The associated requirements can be performed by one or more individuals.

1. Integration into operations and tactical employment of the system, including training.
2. Maintenance and management of biometric WATCHLISTs.
3. Replication of the BAT database as described in paragraph 5 and BAT SOP Part II, Appendix B.
4. Integration and sustainment on the tactical communications network, including system administration for clients on and off the tactical network.
5. Sustainment of the system for maintenance and consumables (such as for badging operations).

**Battalion level operators.** At the battalion level, BAT uses designated operators unless dedicated operators are determined essential by unit requirements (such as detention center enrollment operators). The list may define operator requirements performed by the same individual.

1. Network database manager - designated individual who ensures disconnected BAT clients are updated on a regular basis and that locally networked BAT clients are replicating as discussed in paragraph 5 and BAT SOP Part II, Appendix B. This skill does not require a communications (06XX or 25 series) MOS.
2. Database / WATCHLIST manager – designated individual who ensures local targeting and HVI's are incorporated into the biometric WATCHLIST as discussed in paragraph 4 and BAT SOP Part II, Appendix B. Capable of using BAT for intelligence analysis as well.
3. BAT Operators- designated individuals capable of conducting enrolling, screening, and badging operations, as well as maintaining BAT equipment.

## **2.B. Training.**

Training for BAT and HIIDE is primarily provided by FSE's and the one dedicated trainer for MNF-W. It is coordinated by MSC/MSE's who forward requests to the MNF-W IMO section for prioritization. Training includes but is not limited to basic user operations for enrollment and screening procedures, networking and database replication, and WATCHLIST and database management.

The high rotation of units through missions that employ BAT requires a proactive plan at the battalion and MSC level for training prior to execution and in conjunction with unit rotations. Training of a core group of operators for continuity and train the trainer applications is recommended.

**Reference materials.** Very good reference materials are available on two CD's and also BAT clients. Any individual following the slides and documentation will be able to perform basic operations including WATCHLIST management. What are not provided in training materials are the concepts for employment.

1. BAT Training Materials Version 4.0.4. 24 Jan 2007- includes power point presentation and lesson plans on BAT operator and inventory instructions, HIIDE operator instructions, BAT analyst, tactical detention operations, rapid enrollment procedures, and networking ECP computing, interrogator lesson plans

2. BAT 4.0 Documentation CD 4.0.4.1 6 February 2007- Specific information on the current version of BAT version 4.0. (Subsequently upgrading to Versions 4.0 sp5, with BAT version 5.0 scheduled for release in Fall 2007)
3. The appendices in this SOP provide MNF-W specific TTP's. Additional information including briefs, badge templates, and training schedules are found on the MNF-W BAT HIIDE Portal [www.mnf-w.usmc.smil.mil](http://www.mnf-w.usmc.smil.mil) under the IMO's section.

### **2.C. Handling Classified Material and Foreign Disclosure.**

**Protection of Biometric Data.** Protecting MNF-W biometric data must always be consideration in the development of operational functions. The management and protection of biometric data in a distributive networked environment is a privacy, security, and asset protection necessity. It is critical to protect the integrity of biometric files to maintain the credibility of the authoritative source. **It is critical that US and other Coalition Forces, US citizens, and US contractors not be enrolled in the BAT system,** (If a U.S. citizen is an enemy combatant, seek SJA or PMO for further guidance prior to enrolling).

#### **Destruction of BAT Database/media in the event of a threat**

Personnel will be trained on how to destroy BAT database/media equipments in case of a threat of enemy taking control of the BAT equipment. The basic procedures are pulling the hard drive out of the BAT laptop and destroy the media by any means possible.

**Foreign Disclosure Guidance.** There are two forms of disclosure regarding biometrics. The first is tactical information based on ALERT status. The second, and much more complex, is the release of biometric information.

Unit Foreign Disclosure Officer's are required to authorize disclosure in accordance with standing policies and procedures. Once approved, the technique for disclosure of ALERT information is kept in simple terms.

- He's an Iraqi bad guy (in reality Former Regime, Detainee, AQIZ, 1920, etc.).
- He's an 'external' bad guy (foreign fighter).
- He is a low-level criminal.
- He is a local citizen

Sharing of biometric information within the Iraqi Theater of Operations requires MNF-W coordination with CDRUSCENTCOM. Any requests to share biometric information will be coordinated by the MNF-W IMO and G-2 FDO.

### **3. Operations.**

Specific TTP's for employing the system are located in BAT SOP Part II, Appendices C through M.

#### **3.A. Population Control.**

The BAT system can be used for controlling access to areas and denying AIF freedom of movement by enrolling and badging the local populace. Priorities for

registration of the population groups is determined by the local unit but can include women, local government or tribal officials, workers (such as taxi or truck drivers), or certain age groups.

BAT badges provide an effective means of screening those who are already enrolled in BAT – they can be forged as can any badge, except for the bar code and the number, which a BAT operator can use to screen the individual and determine ‘Go’ or ‘No Go’ in less than 5 seconds.

Badging operations should incorporate Civil Affairs and Information Operations plans. The average time to completely screen, enroll, and badge one individual is between 6-10 minutes.

**3.B. Screening.** Screening identifies if someone exists within the BAT database and also provides identity verification. It is not absolute. Matches can require additional verification depending on what device is used and if multiple matches occur. It is important that new operators realize a match just means that someone is in the system and possibly matched. Verification prior to detainment or other actions is standard practice.

Screening can take two forms- 1) It can confirm that an individual is not in the database (such as confirming someone is not previously enrolled, or not on ALERT). 2) It can confirm that the individual is who they are (by using the badge or a biometric to retrieve their record from the database and then confirming the information).

Screening can be performed by a BAT system with its peripherals attached, by the Pier 2.3 iris scanner when it is detached, or by the HIIDE. Each has different capabilities and the following MNF-W standards are based on speed and accuracy.

**UNCLASSIFIED – FOR OFFICIAL USE ONLY**

<b>BAT Screening</b>					
<b>Methods (Order of preference)</b>	<b>Capability</b>	<b>Speed (when not online)</b>	<b>Accuracy</b>	<b>Equipment</b>	<b>Remarks</b>
<i>BAT-using a bar code scanner</i>	<i>Retrieves an individual record from the entire DB</i>	<i>2-3 seconds</i>	<i>1:1 match of the record. Does not confirm identity</i>	<ul style="list-style-type: none"> <li>• <i>BAT Laptop</i></li> <li>• <i>BarCode Scanner</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Requires a badge.</i></li> <li>• <i>Badge can be typed in manually.</i></li> <li>• <i>Requires visual facial recognition.</i></li> </ul>
<i>Pier 2.3 Iris scanner with the ALERT list loaded</i>	<i>Matches an iris against the entire MNF-W ALERT list (100,000 max)</i>	<i>2-3 seconds</i>	<i>98% accuracy of biometric match</i>	<ul style="list-style-type: none"> <li>• <i>Pier 2.3 Iris Scanner</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Only right irises are loaded.</i></li> <li>• <i>Marine scans both eyes for the 'military left' factor.</i></li> </ul>
<i>HIIDE- Iris scanner</i>	<i>Matches an iris against the loaded list (e.g. NGIC and local watchlist (10,000 max))</i>	<i>2-3 seconds</i>	<i>98% accuracy of biometric match</i>	<ul style="list-style-type: none"> <li>• <i>HIIDE</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Limited number of records.</i></li> <li>• <i>Effectiveness depends on accuracy of the local unit's WATCHLIST</i></li> </ul>
<i>BAT- using an iris scanner</i>	<i>Matches an iris against entire DB</i>	<i>2-3 minutes</i>	<i>98% accuracy of biometric match</i>	<ul style="list-style-type: none"> <li>• <i>BAT laptop</i></li> <li>• <i>Pier 2.3, or Pier T, or HIIDE</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Prerequisite for enrolling and badging.</i></li> </ul>
<i>HIIDE- Finger print Scanner</i>	<i>Matches prints against the loaded list (e.g. NGIC and local watchlist (10,000 max))</i>	<i>3 seconds</i>	<i>70% accuracy of a biometric match</i>	<ul style="list-style-type: none"> <li>• <i>HIIDE</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Good for confirming suspect HVI's.</i></li> <li>• <i>NGIC WATCHLIST John Doe prints</i></li> <li>• <i>Enrolling KIA prints</i></li> </ul>
<i>BAT using a finger print scanner</i>	<i>Matches prints against entire DB</i>	<i>10-15 minutes</i>	<i>70% accuracy of biometric match</i>	<ul style="list-style-type: none"> <li>• <i>BAT laptop</i></li> <li>• <i>Cross Match 300 (or other finger print device)</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Prerequisite for enrolling and badging.</i></li> <li>• <i>Good second verification.</i></li> </ul>

**ECP's.** Screening for controlling access to an area can use both forms of screening. It is imperative that commander's guidance be provided to determine what level of screening occurs at an ECP as well as when and with what frequency. Clarity is essential for effectiveness.

Absolute positive control requires confirming that 100% of all personnel are in the database (requires scanning BAT badges or screening irises while attached to a BAT).

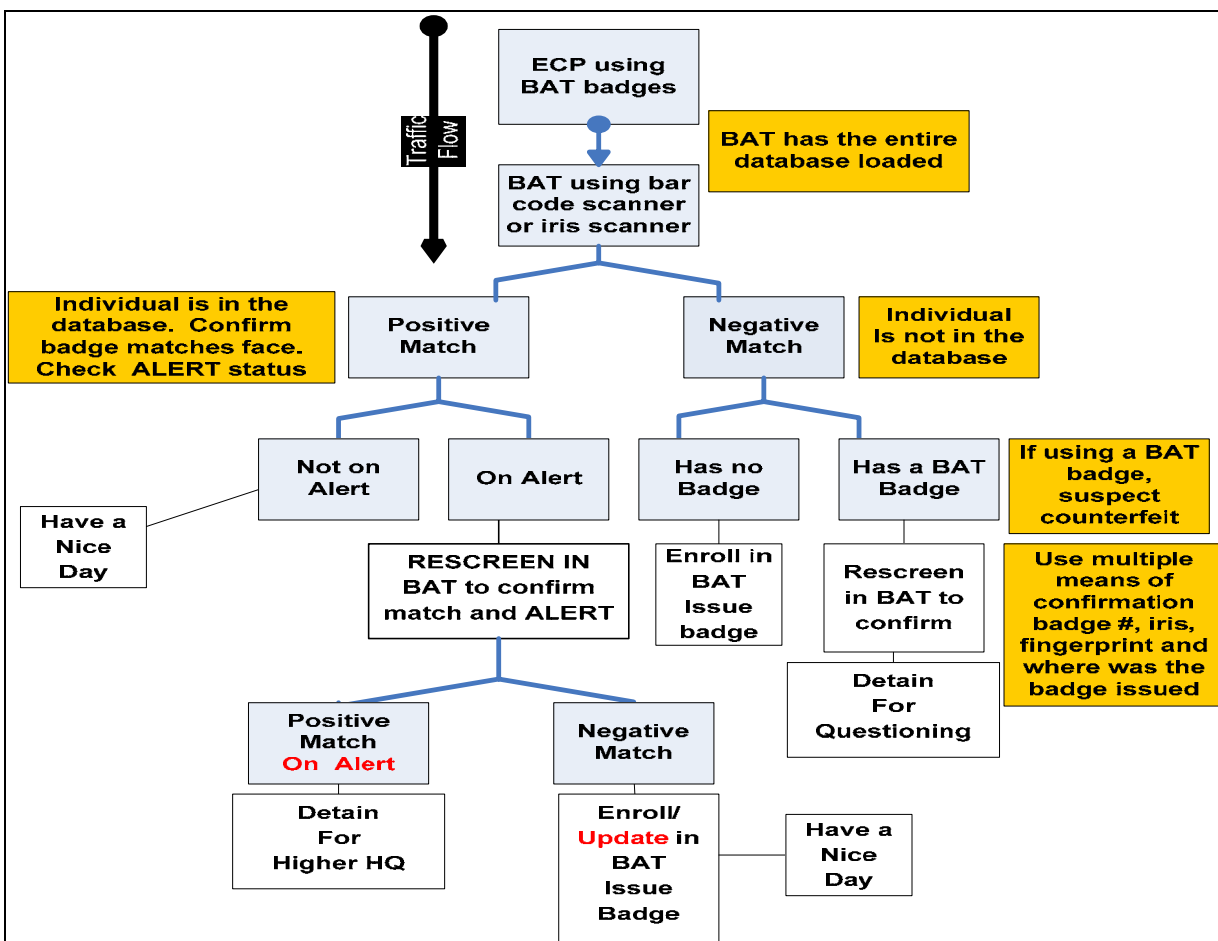
## UNCLASSIFIED – FOR OFFICIAL USE ONLY

The second means of screening is a combination of positive control and only screening for individuals on ALERT or WATCHLIST. The difference from above is the speed of scanning irises for those without badges compared to using an iris scan to retrieve the BAT record from the database. The gain of speed and throughput is offset by not forcing individuals to enroll.

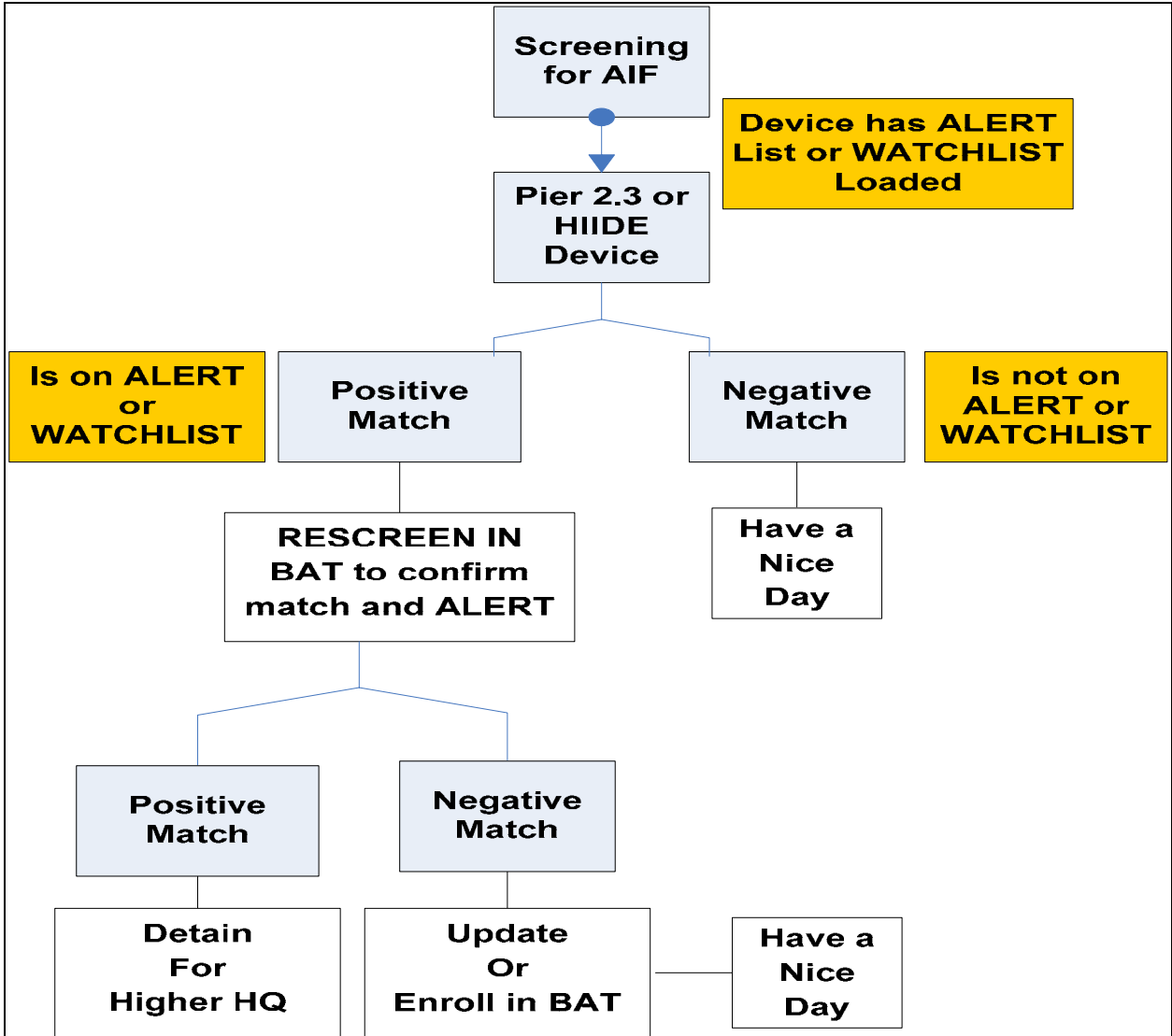
The two forms of screening equate to different actions taken by Marines:

- 1) If screening badges at an ECP a negative response means a person is not in the database and needs to be enrolled or is potentially holding a counterfeit badge.
- 2) If screening irises with either the entire ALERT list or a WATCHLIST, a negative response means the individual is not a previously enrolled, wanted individual.

One additional variable in screening is the number of individuals screened. The standard is every individual gets screened. Only unit commanders on the ground can determine if the deterrent effect of random screening in order to increase throughput outweighs the risk of missing a wanted individual or prevents AIF from attempted infiltration through an ECP.



**Screening for suspected AIF, Snap TCP's and VCP's.** Screening is used to interdict LOC's and deny freedom of movement to insurgents. In these instances it is used to confirm if individuals are on ALERT or a WATCHLIST (depending on the device used). It can also be used to positively confirm the identity of individuals. Systems can be employed for vetting transients in conjunction with large operations (those leaving an area of operation) or in normal daily operations.





MNF-W Standard for screening.

- *Unit commanders will provide guidance to establish the level of screening that occurs at ECP's (this includes variations of type, frequency, and timing).*
- *The fastest and most effective means of screening at ECP's is a bar code scanner using badges with recognition that the person's face matches the BAT record. (The BAT record # in the upper right hand of the badge can also be manually typed in.)*
- *The second most effective means is using an iris scanner in either attached and detached modes (see table below- attached is slower but checks the entire database, detached is very fast but checks only the ALERT list)*
- *For screening for individuals on ALERT, the Pier 2.3 holds the entire ALERTLIST.*
- *For screening for individuals on a WATCHLIST, the HIIDE can hold up to 10,000 records.*
- *The HIIDE can also confirm the identity of friendly personnel when loaded with those records.*
- *Screening to confirm a person is enrolled in the database requires checking against the entire database.*

**3.C. Enrolling.** Enrolling individuals is required to positively identify individuals. Screening to see if an individual already exists in the database is a prerequisite to enrolling, and enrollment is required prior to badging. A successful program requires verification of personal documents, trained operators, and consistency to ensure a good capture of biometric data. Quality enrollments- especially fingerprints, help match AIF with existing records. Biometric enrollment can be conducted at detention facilities, badging centers, ECPs.

MNF-W Standard for Enrolling.

- *Biometric enrollment standards for populace and ISF badging operations- 2 irises, 10 fingers, and a front facial picture.*
- *Textual Data must at least include name, tribe, National ID# (GENSIA), personal data to include birthplace and city/village for address.*

**Vehicle Registrations.** If BAT is used to identify vehicles with approved individuals, there are In addition to the standard fields, the VIN of the vehicle should be listed under 'description'.

**3.D. Badging.** Badges primarily accomplish two things. It verifies someone is already in BAT, and it speeds up verification at screening stations. A badge can be forged, but the bar code cannot. Units must ensure that the populace they give badges to be screened against the most recent database and those credentials are not forgeries (see Part II

Appendix B). Never create a badge without first enrolling the basic biometrics listed above.

MNF-W Standard for Badging.

- Badges are listed in Appendix B
- A GENSIA with a rations card is the basic credential for verifying residency or proof of identity.
- The general guideline is for men 14-65 years.

Units will not create their own badges for their local area. ISF badges made by BAT are utilized in lieu of GOI badging systems; however they meet the MNC-I standard. Badges used for local access to MNF-W bases where BISA does not exist will meet the MNF-I standard.

Any modifications to MNF-W standard badges, such as civilian populace badges with the “authorized weapon in civilian attire” must be approved by MNF-W IMO. (MNF-W standard badges now include a separate weapons cards- see Appendix B.)

**3.E. ISF Recruiting.**

Screening and enrolling ISF recruits accomplishes three things. First it allows us to deny AIF attempting to infiltrate the ISF. Second it allows us the ability to confirm the identity of those joining the ISF. And lastly it provides a convenient means of badging the ISF until MOI and MOD systems come on line.

Where ISF BAT screening, enrolling, and badging takes place is situational dependent. However applicants should at least be screened prior to departing for training to maximize the limited resource of boat spaces. Applicants with negative information are not necessarily disqualified and require guidance for mitigation provided by G-3 ISF.

**3.F. Detainee Operations.**

**Detainee operations at the local unit holding facility.** Detainees can be screened by any BAT system available at the unit level to determine if they are on alert. Units should make every attempt to ensure the BAT used at a local unit holding facility is networked to be constantly updated or is frequently updated by manual means discussed in paragraph 5 and Appendix B.

Every detainee held at the local level should be screened. Detainees forwarded to the RDF that are not already in BAT should **not** be enrolled prior to delivery. However, detainees not forwarded to an RDF and released **should** be enrolled or updated in BAT to reflect the information associated with the local detainment. See Entering data in Paragraph 4.

**Detainee operations by training teams (TT's).** Based on system availability, Mitt's and PTT's can screen personnel detained by Iraqi forces. Due to the system's classification, it can only be employed by US forces and the information requires consideration for disclosure. The biometric data itself is UNCLASS, the textual data is

usually only sensitive but can be CLASSIFIED. The general disclosure TTP for relating screening results to partnered forces:

- He’s an Iraqi bad guy (Former Regime, Detainee, etc.)
- He’s an ‘external’ bad guy (Foreign Fighter)
- He is a low-level criminal
- He is a local (MNF-W) resident

**Detainee operations at the regional detention facility (RDF).**

**Enrolling detainees.** RDF’s have established internal procedures for screening and enrollment. In addition to the standard enrollment for residents (both irises, all fingers, and facial photo) detainees enrollments will include fingerprint slaps / rolls, and facial profile pictures from the side and 45 degree angle. The BAT training document has training materials for detainee enrollment procedures.

**Updating status for detainees.** Prior to physically leaving an RDF, all detainees will be scanned biometrically in order to confirm identity and check for any recent updates in the BAT database- specifically recent published biometric matches (BIARS) or other alerts. BAT entries related to transfer/release will be one of the three categories.

1. Transferring to another facility and still in custody- Individual stays ON ALERT (due to number of unknown releases and escapes).

TEXT-“**Transferred to X. Under custody**”. (Duplication of detainee tracker but this is for the user at the ECP who encounters this individual if he wanders before completing his sentence)

2. Released back into public but we would like to have prosecuted or held - Individual stays ON ALERT and text explains he is considered a threat but not currently wanted.

TEXT- **Use caution- Detained for X and released due to inability to prosecute. Not currently wanted.**

3. Released due to insignificant evidence and not considered a threat to CF- Individual is taken OFF OF ALERT, enter circumstance in X field.

TEXT- **Previously detained and released for X. No indications of AIF involvement.**

*MNF-W Standard for Detainees.*

- *Local units will only enroll or update detainees that are **NOT** forwarded to the RDF.*
- *RDF detainee enrollments will include fingerprint slaps / rolls, and facial profile pictures from the side and 45 degree angle.*

### **3.G. HVI, AIF Target Confirmation (including KIA)**

The prerequisite for using biometrics to confirm the identity of an HVI is that they are already enrolled in BAT. However, captured or killed AIF can be enrolled or screened against the database. While the iris quickly and more accurately identifies an individual, fingerprints of suspected AIF can be matched against possible John Doe finger prints which currently exist or may be entered in the future.

KIA enrollments. In cases where forces have the opportunity to screen or enroll enemy combatants who are KIA, it provides the opportunity to definitively identify AIF personnel and remove them from the targeting process as well as conduct intelligence analysis.

Iris screening and Fingerprint enrollment can be conducted by either the BAT or HIIDE system. This is one of the few acceptable instances of using a HIIDE to create an enrollment. BAT is still the preferred system if available.

Both irises and finger prints should be collected. Irises are scannable up to four hours after death and fingerprints within eight hours depending on the environment.

*MNF-W standard for suspected screening AIF.*

- *Attempt to screen all suspected AIF. Whenever feasible KIA will be screened and or enrolled in either BAT or HIIDE.*

**3.H. Base access and local security.** In locations where base access includes BAT systems for screening local nationals as well as third country nationals, the effort must be coordinated and complementary with BISA and or other systems.

Where BISA is used, local hires will still be screened and enrolled in the BAT database for intelligence purposes. Future developments by Dec 2007 will provide information from BISA LEP screenings to populate BAT files.

*MNF-W Standard for BAT badges used for base access.*

- *Badges for base access made using BAT should follow the BISA appearance standards.*

**Base access using HIIDE.** When using HIIDE to confirm local nationals approved for access, **database managers** will designate which systems contain HVI data and those that contain worker biometric data via color coded sticker/tape. “Red” is HVI/POI and “blue” is base/camp worker.

### **3.I. HIIDE Employment Considerations.**

The HIIDE is primarily used for screening based off of a WATCHLIST loaded from the BAT database. The WATCHLIST can be for known or suspected AIF to be detained or for confirming the identity of known friendly personnel such as government officials or local nationals. For WATCHLIST procedures see Para 4 and BAT SOP Part II, Appendix A.

HIIDE will only be used for enrolling personnel that cannot be enrolled in normal badging operations; e.g. personnel at a raid target site, corpses, or suspected AIF that will not be enrolled through the normal detainee process. Coordinate with MNF-W IMO prior to execution of missions with HIIDE enrollments.

MNF-W Standard for HIIDE employment.

- HIIDE WATCHLIST's for known or suspected AIF will be updated at least every 7 days.(see para 4 for WATCHLISTs)
- HIIDE will only be used for enrollment when individuals will not foreseeable

#### **4. Database Management**

**4.A. ALERT Status and Entry Management.** In order for BAT to be effective, units have to manage the information in the database. A basic requirement is appointing an information manager who has overall responsibilities for what information is entered and extracted from the system. He should also:

1. Establish standards for what information is entered on dossiers—whether through badge enrollments, detainees, or local targeting efforts.
2. Establish who has authority to put someone on, or take them off of ALERT.
3. Screen local records for quality control and corrections.
4. Ensure the local WATCHLIST is integrated into the targeting cycle.

**The BAT database.** The BAT database includes personnel dossiers, biometric data, and attachments which include intelligence records. The database includes the entire profile of personnel enrolled by DOD. Unless a unit is using the network on a major FOB, their BAT database will not include intelligence attachments and is called a 'skeleton record' database.

The database is only as good as the information placed in it. Operators often find errors and incomplete information. Unsupervised operators will continue to make additional errors and incomplete records. Whenever possible, correct errors that are encountered without deleting existing information. Unit operators need standards and consistency to be as complete as possible in providing information that other users can understand.

**ALERT Status.** The most important information in a personnel dossier is whether a person is on ALERT and what is entered in the ALERT text field. The ALERT tag provides BAT or HIIDE operators an immediate notification of special information on an individual. Personnel on ALERT in the database have their record and photo outlined in red (pink when selected). Note that the Pier 2.3 iris scanner only provides the first 16 characters of the ALERT field text. The reason for ALERT should be enduring and will be valid for years to come as the database is used. An individual can be on ALERT for various reasons.

1. Wanted for detention by coalition forces (NGIC/MNF-W Tier 1HVI's, prison escapees, known or suspected AIF)
2. Warning CF of previous detention (if possibly dangerous but not wanted for detention).

3. Administrative such as an expired BAT badge or incomplete biometrics (missing irises or fingerprints).
4. Previously on ALERT for unknown reasons, but never removed.

**Note-** There is previous detainees who are not on ALERT that may or may not be a threat due to inaccurate reporting. They also may be associated with friendly forces now in support of CF.

*MNF-W Standard for ALERT entries.*

1. *Units will establish specific personnel authorized to place an individual on ALERT.*
2. *Units will use the established procedure, including specifying an approval authority, to remove someone from ALERT.*
3. *Units are not authorized to remove ALERTS or alert text from NGIC, MNC-I, MNF-I based entries.*
4. *Alert text should provide POC, DSN/SVOIP numbers for verification and action.*
5. *ALERT text will start the most important words or verb to convey action required:*
  - *DETAIN, USE CAUTION, UPDATE DATA, DO NOT RELEASE, DENY ACCESS*

**Correcting inaccurate records.** Units will encounter individuals who are incorrectly on ALERT or have no discernable entries. In order to remove from ALERT the following procedure is required.

1. Cross-reference Detainee Tracker and / or other HUMINT systems.
2. Obtain unit approving authority (SNCOIC or S-2 representative).
3. In the Alert text field enter—PREVIOUS ALERT FOR UNKNOWN REASONS, DO NOT DETAIN UNLESS FOR CAUSE.

**Ways to tell if someone was previously detained but not on ALERT.**

- Photo in an orange or yellow jumpsuit.
- Attachments include profile photos or handprints (RDF full enrollment).
- Attachments include G-2/S-2 documents.
- Cross reference Detainee Tracker (on the MNF-W G-2 TFC web portal).

**4.B. WATCHLIST MAINTENANCE & MANAGEMENT.** A biometric WATCHLIST is a list of individuals who are on ALERT, who has had biometrics collected on them, and need to be detained when encountered. They are considered either a threat, intelligence value, or both. There are several different WATCHLISTs.

**The NGIC Biometric WATCHLIST** is a biometrically-based repository of information to identify persons assessed as a threat to CF, and to the national security of the United States. It includes High Value Individuals (HVIs), High Value Targets (HVTs) or Persons of Interest (POIs) within MNF-W.



**Local WATCHLISTs** consists of HVIs and POIs that are not on the NGIC WATCHLIST. Examples include the MNF-W WATCHLIST, the AO RALEIGH, AO TOPEKA, and AO DENVER WATCHLISTS (note MSC WATCHLISTS are not identified by unit but by area of operations).

**WATCHLIST Purpose.** The purpose of a WATCHLIST is to provide a subset of the ALERT list that is maintained specifically for targeting and related to the targeting cycle for a unit or geographic area. WATCHLISTs are essential for units employing HIIDE, because the system cannot contain the entire ALERT list. Well-maintained WATCHLISTs ensure the right biometric records are available for screening suspected AIF.

**WATCHLIST Management.** The management of local WATCHLISTs has to be integrated into the targeting cycle. In simple terms a unit uses its targeting list to search the BAT database for any biometric records to place on the WATCHLIST. It requires maintenance to the continual addition, and deletion of records to produce the most current WATCHLIST. Detailed procedures are in Appendix A.

*MNF-W Standard for WATCHLISTS.*

- *Each RCT/BCT and battalion will assign a watchlist manager within its intelligence (S-2) section.*
- *Watchlist maintenance will occur weekly within the normal targeting cycle from the Company to the MEF level.*
- *MNF-W will use standardized watchlist naming conventions in BAT SOP Part II, Appn A to prevent HVI's or entire lists from being omitted when searched.*
- *MNF-W WATCHLIST nominations will be reflected in the NGIC WATCHLIST*

## **5. Database Replication and Communications Networking**

**5.A. Database Replication.** BAT is not effective if the database cannot be kept up to date with new enrollees and those placed on ALERT. Units must have a database 'replication' plan in order for BAT clients to maintain the up to date information on ALERTs and new records. Each BAT client holds the entire database of personnel entered in the system if not connected to a server, so each BAT location has to be integrated into the communications/networking plan, even if disconnected and being physically updated. This is discussed in detail in BAT SOP Part II, Appendix B and coordinated by the unit S-6 to maximize the efficiency of the tactical network.

**Three ways to access the BAT database:**

1. Stand alone: A disconnected client accesses the records on its hard drive. This contains the entire DB (approximately 600,000 records) and is affected by how long the system has or has not been updated.

2. Local Server: A local client can be networked (connected to a local server (another BAT can act as a server)) using a LAN. This is common with badging operations, where there is multiple BAT located, or within a COC.
3. Online: A BAT can be connected like any other SIPR computer to the tactical network to access a BAT server close by or one of the main servers located on a distant FOB.

**Updating the database** occurs two ways:

1. Replicating files over the network (tactical communications network or local LAN) using a program called DSS.
2. Synchronizing files by a connected client (preferred) or an external hard drive (slower) brought to the site. This is referred to as the sneaker net.
  - a. The sneaker net can be accomplished by bringing the BAT Client to the battalion to enable the unit POC to perform a manual database update for the client or having the battalion POC travel to different BAT client locations.
  - b. It can also be performed by bringing the BAT client to the closest BAT FSE to update the database.

*MNF-W Standards for Replication.*

- *Units will have a replication plan for updating their BAT clients databases. This includes MTT's, PTT's, and BTT's.*
- *Units not located on major FOBs will only maintain and replicate the 'skeleton database.' (Battalion intelligence sections still have the ability to download individual attachments on individual as needed via SIPRNET.)*
- *Order of precedence for updating the database at the Battalion and below is replication from a single point to a single BAT client/server that then can be networked, then physical synchronization using a connected BAT client, then physical synchronization using an external storage device.*
- *The standard for updating disconnected clients is daily (ideal), less than 96 hours (objective), but at least weekly (minimum). (The exception to this is designated units separated by large geographic distances in AO Denver).*
- *Disconnected clients that are conducting enrollment operations should be updated daily unless in conjunction with a short duration operation without communications support.*

**5.B. Communications Networking.**

**Replication over the tactical network.** At present, database replication rates are limited to a maximum of 128 KB (1.3 Mbps for transmission links) by the BAT operating system/software. Database replication can and will occur at lower data rates but at a commensurate increase in time required for completion. With the soon to be released update to the BAT operating system/software (DSS 2.7), this limitation on replication rates will be removed. This may cause replication plans to be modified, but is expected to bring overall efficiencies to the system. Units should maximize off hours in



synchronizing clients from 2200-0600 and use comparisons of the total records in each BAT client to determine whether replication is being effectively accomplished.

**Synchronizing by physical transfer of data.** Units may have to physically transport data to update their BAT systems via the sneaker net. Whether units bring the disconnected BAT to a server or data is brought to the BAT, there are efficiencies in how this is accomplished.

1. A BAT that is updated less than <96 hours from its last update only exchanges data from the last 96 hours on both systems (must faster and still accurate if using the same two systems). More than 96 hour synchronizations can take from 6-10 hours.
2. A BAT synchronizes much faster when connected to another BAT vice an external drive.
3. If multiple systems are being synchronized at once, a local network (a small router or layer 3 switch) is effective.

## **6. Equipment Supply, Maintenance and Sustainment**

**6.A. Supply Concept.** Both BAT and HIIDE are Special Equipment Items (SEI). Both items are considered sensitive; however the BAT hard drive is CLASSIFIED SECRET and must be accounted for as such (see Para 2C). When a HIIDE is loaded with a WATCHLIST it is considered UNCLASSIFIED FOUO.

Receiving new or replacement systems will be received through the MLG SMU Initial Issue Point. This will ensure centralization of assets and sole source identification for when new systems arrive. The SMU IIP will notify the MNF-W G4 Supply Officer upon receipt, keeping with current practices, and reducing opportunity for mid-identification and transfer to non-BATS commodity managers.

Fielding of new equipment will typically be initiated by one of two ways. Either the MNF-W IMO will provide distribution instructions to fill shortages, replace losses, or increase unit capabilities, or using units will request additional machines due to changing CONOPS in their respective AOR's.

MNF-W G-4 Supply will provide distribution instructions via email or naval message to the IIP, establishing the source document for transfer of BATS/HIIDE systems to the gaining unit(s).

The IIP will conduct a Z2M redistribution transaction to ensure asset visibility throughout the transfer process. The gaining unit will receipt for the system and place on the appropriate CMR. Completion of receipting action will be via naval message back to MNF-W G4 Supply.

Unless otherwise notified through official correspondence, at NO TIME, will any components of the BATS/HIIDE suite of systems become associated with the A9100 MCHS, Computer GP, laptop, or any other computer or optics system.

**UNCLASSIFIED – FOR OFFICIAL USE ONLY**

When BATS/HIIDE systems enter the maintenance cycles, owning units will retain accountability for the asset, by serial number, unless directed to rollback, or upon receipt of disposition instructions.

Transfers within the owning unit should be executed via normal chain of custody/CMR procedures.

Transfers to non-organic units will only be executed upon receipt of official traffic from MNF-W G4 Supply.

<b>TAMCN</b>	<b>NSN</b>	<b>Nomenclature</b>
A0028	9999015314667	BAT COMPUTER, w/ Camera, Iris Scanner, Fingerprint Scanner, Carrying case
HL328	7510-01DTQ-1019	PRINTER, BAT DTC-400
HL328	7510-01DTQ-1020	PRINTER, BAT DTC-525L
HL0482	7050-01DTQ-0246	TEN-PRINT FINGERPRINT SCANNER
A01687G	5895-01-545-3002 ID# 11369A	IDENTITY DETECTION EQPMT, HANDHELD

<b>Mobile/Disconnected Operating Hours</b>		
<b>Device</b>	<b>Estimated</b>	<b>Power Source</b>
BAT Laptop	3-4 Hrs	Internal Battery
Camera	2 hrs	AA Battery
Pier 2.3 Iris Scanner	3-4 Hrs	Internal Battery
HIIDE	3-4 Hrs	Internal Battery
Bar-Code Scanners	N/A	Laptop
CrossMatch 300	N/A	Laptop

<b>Power Requirements</b>		
<b>Device</b>	<b>Voltage</b>	<b>Amps</b>
BAT Laptop	100-240	1.7A, .75A
Camera	100-240	16VA, - 26VA
Pier 2.3 Iris Scanner	100-240	.8A
HIIDE	100-240	1.7A
External Hard Drive	100-240	.65A
Badge Printer (DTC 400)	100-240	1.9A

**6.B. Maintenance.** Both BAT and HIIDE systems are covered by warranty and any corrective maintenance is performed by contracted logistic support. Gear is evacuated through normal channels to the Combat Logistics Battalion (CLB). A separate service contract is in place for U.S. Army procured BAT/HIIDE systems so units or FSR's need to ensure they're aware of the origin for a particular system, before sending off for maintenance.

**Steps for evacuation and replacement non-repairable BAT equipment under warranty:**

1. Gear malfunctions- Local unit contacts FSE (CF, AR, and AA) available via VOIP or email to troubleshoot prior to evacuation. (This also serves to notify FSE that gear is down to begin coordination of replacement with owning MSC.)
2. Owing Unit will open an equipment repair order (ERO) for physical custody and receipt and evacuate through unit organic maintenance to CLB.
3. Account for classified using CLASSIFIED handling procedures (utilize SF -153 for any transfer of classified). Failed CLASSIFIED hard drives are held by owning unit for accountability and destruction.
4. The ICE2 maintenance FSR's at CLB's will coordinate with local BAT FSE's to determine if gear is US Army TPE or USMC in order to forward to the appropriate agency (GISA for USA; ICE2 for USMC) and whether replacements are available.
5. A replacement will be provided if available. Serialized gear will be issued on a DD1348. Owing MSC's will allocate resources within the CLB's stock and MNF-W IMO will have overall authority for allocation of resources.
6. Units requiring system FSE support (reloading of databases) are DIRLAUTH for coordination with the local FSE.
7. Repaired items will be replaced in the ready supply chain as a replacement item at the ICE II facility.

**HIIDE Maintenance and Evacuation.** HIIDE is evacuated using the same procedures. Most users never create a Key and so only need to clear the system of its data. However, prior to evacuation if Marines have created a key will have to execute the "Destroy Key" function and open ERO and evacuate through organic maintenance via the CLB. The responsible officer and unit Classified Material Control Center (CMCC) Custodian will ensure no data is present on the HIIDE before entering it into the maintenance cycle.

**6.C. Sustainment.** The consumable items associated with BAT operations include badging printer ribbons, cleaning kits, and the badges themselves. Each is available through the unit supply chain and is stocked in the SMU or available through open purchase.

**UNCLASSIFIED – FOR OFFICIAL USE ONLY**

Item	Manufacture Part#	Unit of issue
Fargo 400 Printer Ribbon YMCKOK	44240	Each
Fargo 550 Printer Ribbon YMCOK	86200	Each
Color ID blank Plastic Badge	CW103000	Box of 500

Cleaning kits for fingerprint scanners can be ordered through the Crossmatch website, [http://www.crossmatch.com/accessories\\_and\\_supplies.html](http://www.crossmatch.com/accessories_and_supplies.html) . Part # 900232 (Guardian Supplies, \$400), part # 900225 (Verifier 300 Supplies, \$150) and part # 900227 (ID 500 Supplies), \$400).

**Appendix A. MNF-W Standards.**

MNF-W Standard for billets.

- Units employing biometric systems will designate an officer or SNCO responsible for the overall employment of the system.

MNF-W Standard for screening.

- Unit commanders will provide guidance to establish the level of screening that occurs at ECP's (this includes variations of type, frequency, and timing).
- The fastest and most effective means of screening at ECP's is a bar code scanner using badges with recognition that the person's face matches the BAT record. (The BAT record # in the upper right hand of the badge can also be manually typed in.)
- The second most effective means is using an iris scanner in either attached and detached modes (see table below- attached is slower but checks the entire database, detached is very fast but checks only the ALERT list)
- For screening for individuals on ALERT, the Pier 2.3 holds the entire ALERTLIST.
- For screening for individuals on a WATCHLIST, the HIIDE can hold up to 10,000 records.
- The HIIDE can also confirm the identity of friendly personnel when loaded with those records.
- Screening to confirm a person is enrolled in the database requires checking against the entire database.

MNF-W Standard for Enrolling.

- Biometric enrollment standards for populace and ISF badging operations- 2 irises, 10 fingers, and a front facial picture.
- Textual Data must at least include name, tribe, National ID# (GENSIA), personal data to include birthplace and city/village for address.

MNF-W Standard for Badging.

- Standard Badges are listed in Appendix B
- A GENSIA with a rations card is the basic credential for verifying residency or proof of identity.
- The general guideline is for men 14-65 years.

MNF-W Standard for Detainees.

- Local units will only enroll or update detainees that are **NOT** forwarded to the RDF.
- RDF detainee enrollments will include fingerprint slaps / rolls, and facial profile pictures from the side and 45 degree angle.

MNF-W standard for suspected screening AIF.

- Attempt to screen all suspected AIF. Whenever feasible KIA will be screened and or enrolled in either BAT or HIIDE.

MNF-W Standard for BAT badges used for base access.

- Badges for base access made using BAT should follow the BISA appearance standards.

MNF-W Standard for HIIDE employment.

- *HIIDE WATCHLIST's for known or suspected AIF will be updated at least every 7 days (see Para 4 for WATCHLISTs).*
- *HIIDE will only be used for enrollment when individuals will not foreseeable be enrolled any other way.*
- *HIIDE used for screening for suspected AIF will at least load the NGIC WATCHLIST, the SOTF –W WATCHLIST, and the Local AO WATCHLIST.*

MNF-W Standard for ALERT entries.

- *Units will establish specific personnel authorized to place an individual on ALERT.*
- *Units will use the established procedure, including specifying an approval authority, to remove someone from ALERT.*
- *Units are not authorized to remove ALERTS or alert text from NGIC, MNC-I, MNF-I based entries.*
- *Alert text should provide POC, DSN/SVOIP numbers for verification and action.*
- *ALERT text will start the most important words or verb to convey action required:*
  - *DETAIN, USE CAUTION, UPDATE DATA, DO NOT RELEASE, DENY ACCESS*

MNF-W Standard for WATCHLISTS.

- *Each RCT/BCT and battalion will assign a watchlist manager within its intelligence (S-2) section.*
- *Watchlist maintenance will occur weekly within the normal targeting cycle from the Company to the MEF level.*
- *MNF-W will use standardized watchlist naming conventions in Appendix D to prevent HVI's or entire lists from being omitted when searched.*
- *MNF-W WATCHLIST nominations will be reflected in the NGIC WATCHLIST*

MNF-W Standards for Replication.






- *Units will have a replication plan for updating their BAT clients' databases. This includes Mitt's, PTT's, and BTT's.*
- *Units not located on major FOBs will only maintain and replicate the 'skeleton database.' (Battalion intelligence sections still have the ability to download individual attachments on individual as needed via SIPRNET.)*
- *Order of precedence for updating the database at the Battalion and below is replication from a single point to a single BAT client/server that then can be networked, then physical synchronization using a connected BAT client, then physical synchronization using an external storage device.*
- *The standard for updating disconnected clients is daily (ideal), less than 96 hours (objective), but at least weekly (minimum). (The exception to this is designated units separated by large geographic distances in AO Denver).*
- *Disconnected clients that are conducting enrollment operations should be updated daily unless in conjunction with a short duration operation without communications support.*

*Appendix B. MNF-W Standard Badges*





Government Worker with  
Weapon and Without

A L A N B A R  P R O V I N C E	 	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> National ID Number or Gensia: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456 Authorizing Signature: Holders Signature: 	A L A N B A R  P R O V I N C E	 
	F: <b>Lal</b> M: L: <b>Bahadir</b> <b>GOVERNMENT</b> <b>Dog Catcher</b> Expires: <b>16JUN2007</b>	F: <b>Lal</b> M: L: <b>Bahadir</b> <b>GOVERNMENT</b> <b>Dog Catcher</b> Authorized Weapon in Civilian Attire بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ Expires: <b>16JUN2007</b>		

Local Important Person with  
Weapon and Without

A L A N B A R  P R O V I N C E	 	BAT Badge ID Number: <b>53D42325</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> National ID Number or Gensia: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456 Authorizing Signature: Holders Signature: 	A L A N B A R  P R O V I N C E	 
	F: <b>Lal</b> M: L: <b>Bahadir</b> <b>LOCAL LEADER</b> <b>SHEIK/MUHKTAR/IMMAM</b> Authorized Weapon in Civilian Attire بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ Expires: <b>16JUN2007</b>	F: <b>Lal</b> M: L: <b>Bahadir</b> <b>LOCAL LEADER</b> <b>SHEIK/MUHKTAR/IMMAM</b> Expires: <b>16JUN2007</b>		

## Iraqi Army with Weapon and Without






I R A Q I S E C U R I T Y F O R C E	 	F: <b>Lal</b> M: L: Bahadir	<b>IRAQI ARMY</b> <b>Captain</b>	Authorized Weapon in Civilian Attire بِمِمْ بَحْرِن السِّلَاح Expires: <b>16JUN2007</b>	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> Ministry of Defense Number: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456 Authorizing Signature: Holders Signature: 	I R A Q I S E C U R I T Y F O R C E	 	F: <b>Lal</b> M: L: Bahadir	<b>IRAQI ARMY</b> <b>Private</b>	Expires: <b>16JUN2007</b>

## Iraqi Police with Weapon and Without


I R A Q I S E C U R I T Y F O R C E	 	F: <b>Lal</b> M: L: Bahadir	<b>IRAQI POLICE</b> <b>Captain</b>	Authorized Weapon in Civilian Attire بِمِمْ بَحْرِن السِّلَاح Expires: <b>16JUN2007</b>	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> Ministry of Interior Number: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456 Authorizing Signature: Holders Signature: 	I R A Q I S E C U R I T Y F O R C E	 	F: <b>Lal</b> M: L: Bahadir	<b>IRAQI POLICE</b> <b>Private</b>	Expires: <b>16JUN2007</b>



## PSF with Weapon and Without

IRAQI SECURITY FORCE	 	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> National ID or Gensia Number: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456	IRAQI SECURITY FORCE	 
	F: <b>Lal</b> M: L: Bahadir <b>IRAQI PSF</b> <b>Captain</b> Authorized Weapon in Civilian Attire يسمح بحمل السلاح Expires: <b>16JUN2007</b>	Authorizing Signature:  Holders Signature:  		F: <b>Lal</b> M: L: Bahadir <b>IRAQI PSF</b> <b>Private</b> Expires: <b>16JUN2007</b>

## Iraqi Highway Patrol with Weapon and Without

IRAQI SECURITY FORCE	 	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> Ministry of Interior Number: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456	IRAQI SECURITY FORCE	 
	F: <b>Lal</b> M: L: Bahadir <b>HIGHWAY PATROL</b> <b>Captain</b> Authorized Weapon in Civilian Attire يسمح بحمل السلاح Expires: <b>16JUN2007</b>	Authorizing Signature:  Holders Signature:  		F: <b>Lal</b> M: L: Bahadir <b>HIGHWAY PATROL</b> <b>Private</b> Expires: <b>16JUN2007</b>

## Traffic Police with Weapon and Without

I R A Q I S E C U R I T Y F O R C E		BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> National ID or Gensia Number: <b>T944</b> Weapon Serial Number: AK#123456 GLK#123456 Authorizing Signature:  Holders Signature:  	I R A Q I S E C U R I T Y F O R C E	
				
F: <b>Lal</b> M: L: Bahadir <b>TRAFFIC POLICE</b> <b>Captain</b> Authorized Weapon in Civilian Attire بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ Expires: <b>16JUN2007</b>				F: <b>Lal</b> M: L: Bahadir <b>TRAFFIC POLICE</b> <b>Private</b> Expires: <b>16JUN2007</b>

## Resident Populace badge and Non-Resident Worker

F: <b>Lal</b> M: L: Bahadir   <b>FALLUJAH RESIDENT</b>  BAT Expires: <b>16JUN2007</b>	BAT Badge ID Number: <b>A812B123</b> Issue Date: <b>15JUN2007</b> Badge Issuing Organization: <b>Unit Issuing Badge</b> Enrollment Date: 4/10/2004 5:36:35 PM DOB: <b>1/2/1981</b> Sex: <b>MALE</b> National ID Number or Gensia: <b>T944</b>  Authorizing Signature:  Holders Signature:  	F: <b>Lal</b> M: L: Bahadir   <b>NON-RESIDENT WORKER</b>  BAT Expires: <b>16JUN2007</b>
---	---	---

## Local AT/FP Access Badge

 <p><b>V</b> TEMPORARY VISITOR Unit Issuing Badge A812B123 <b>NO ESCORT REQUIRED</b></p>	BAT Badge ID Number: <b>A812B123</b>	 <p><b>V</b> TEMPORARY VISITOR Unit Issuing Badge A812B123 <b>ESCORT REQUIRED</b></p>
	Issue Date: <b>15JUN2007</b>	
	Badge Issuing Organization: <b>Unit Issuing Badge</b>	
	Enrollment Date: <b>4/10/2004</b>	
	DOB: <b>1/2/1981</b> Sex: <b>MALE</b>	
	BAT Badge Number: <b>T944</b>	
	Authorizing Signature:	
	Holders Signature:	
		

## APPENDIX C. SOP for recording badges in BAT

Badges that are made through a BAT system will be recorded and named as described in the following paragraphs.

When a BAT record is open and you are viewing the Personal Data Report, in the **ID Numbers** section is where the badge you just made will be recorded. There are two fields: **ID Number Type** and **ID Number**. ID Number Type will be dictated below; ID Number will be the eight (8) digit letter/number combination on the back upper right side of the badge, which corresponds with the actual barcode on the bottom.

The units that are issuing badges for the local residents will NOT issue a badge to an individual that is not from their respective city. Each area will badge their cities' residents only. This is an attempt to keep the Host Country Nationals from having badges from different cities, especially if they are only a visitor to a particular area, and not a resident. This will also help each individual unit to preserve their badges and ribbons for their AO only.

### 1. ANAH

Districts:

Qadisiyah	Al Shisan
Yarmuk	Nasir
Khathra/Jihad	Al Basia

All cities/villages in the mentioned **districts** will all fall under the naming convention of **ANAH**. In the **ID Number Type** field, **ANAH** will be picked from the drop down list (or typed in if not there).

### 2. CAMP AL ASAD

All **outlying areas** surrounding Al Asad will fall under the naming convention of **AL ASAD**. In the **ID Number Type** field, **AL ASAD** will be picked from the drop down list (or typed in if not there).

### 3. CAMP AL QAIM

Districts:

Al Qaim	South Ubaydi
Ramanah	North Ubaydi

Outlying Areas

Husaybah	Sadah
Sinjik	Al Qaim
Karabilah	Konetra

## UNCLASSIFIED – FOR OFFICIAL USE ONLY

Arabt	Ad Dayr
Bubait	Al Korhe AKA Chidish/Karez
Albu Hardan	Bilaliyah
Khutaylah	Jazzaniyah
As Sammah	Jassiyah
Dughaymah	Ajjimiyah
West Ubaydi (old)	Ammari
East Ubaydi (new)	Baghooz
Beitha	Jraiheb or Juray'jib
Jabareah	Qunatra
Al Romia	Al-Salman (Ramanah)
Bubiyah	Fayadee
Artajah	

All **outlying areas** and the cities/villages in the mentioned **districts** will all fall under the naming convention of **AL QAIM**. In the **ID Number Type** field, **AL QAIM** will be picked from the drop down list (or typed in if not there).

#### 4. CAMP AL TAQADDUM (TQ)

All **outlying areas** surrounding Camp Al Taqaddum will fall under the naming convention of **TQ**. In the **ID Number Type** field, **TQ** will be picked from the drop down list (or typed in if not there).

#### 5. CAMP AL WALEED

All **outlying areas** surrounding Camp Al Waleed will fall under the naming convention of **WALEED**. In the **ID Number Type** field, **WALEED** will be picked from the drop down list (or typed in if not there).

#### 6. FALLUJAH

##### Districts:

Wahda	Bazaar
Jughafi	Andaloos
Shorta	Sina'ee
Dubat 2 (Officers)	Kurd
Askari	Zawiyah
Jolan	Risalah-Jubayl
Jumhuriyah	Tamim-Jubayl
Azragiyah	Jubayl-Jubayl
Dubat 1	Khadra-Jubayl
Sook	Jubayl
Mualimeen	Nazaal
Medaniyeen	Shuhada

## UNCLASSIFIED – FOR OFFICIAL USE ONLY

All cities/villages in the mentioned **districts** will all fall under the naming convention of **FALLUJAH**. In the **ID Number Type** field, **FALLUJAH** will be picked from the drop down list (or typed in if not there).

### 7. HABBANIYAH/KHALIDIYAH

Districts:

Jazirah Farming Area  
Albu Dimnah  
Husaybah  
Sadaqiyah  
Fleiss  
Abu Mari

Shohada  
Camp Habbaniyah  
Civil Camp  
Coolie Camp  
Sinh Abd Dhibban

Outlying Areas:

Al Ghortan  
Al Garahal  
Al Karabilah  
Al Janabi (Albu Assaf)  
Al Hueja  
Al Akrad  
Abu Fleiss  
Al Falayhat  
Al Halabsah  
Al Tabor  
Al Zuwiyah  
Al Malatmah  
Al Shameyah  
Al Matrodien  
Al Khalifa  
Al Mohamdi  
Al Shuhadah  
Al Subayhat  
Al Mishadah  
Albu Bali  
Albu Dimnah

Albu Diab  
Albu Soda  
Albu Hazem  
Albu Hanush  
Albu Shaab  
Albu Jahash  
Albu Aitha (Al Fahama)  
Albu Azzam  
Albu Shaben  
Albu Mari  
Albu Ubayd  
Albu Zion  
Mudiq  
Sadaqiyah  
Husaybah-Sharqiyah  
Spanish Village  
Albu Thiah  
ASP  
Angora  
Sinah Dhibban  
Falahat

All **outlying areas** and the cities/villages in the mentioned **districts** will all fall under the naming convention of **H/K**. In the **ID Number Type** field, **H/K** will be picked from the drop down list (or typed in if not there).

### 8. HADITHAH TRIAD

Districts:

Sheik Hadid  
Thamania

Wadi Hamza  
Rafi

Surai  
Police  
Echo Firmbase  
Market  
Sinai  
Hail Askari  
Hajiria  
Howijah  
Sub Hani

Mechanics  
School  
Communication  
Hill  
Fish Market  
Souq  
Anabi Ferry  
Darasal

Outlying Areas:

Hadithah Dam  
Hadithah  
Haqlaniyah  
Barwanah  
Albu Hyatt

Bani Dahir  
Khaffajiah  
Alus  
Cykla  
Sakran

All **outlying areas** and the cities/villages in the mentioned **districts** will all fall under the naming convention of **TRIAD**. In the **ID Number Type** field, **TRIAD** will be picked from the drop down list (or typed in if not there).

**9. CAMP HIT**

Districts:

Al-Khaldia  
Abu Bashir  
Al-Jamiyah “Association”  
Al-Jazirra  
Fruit Stands  
Butcher Area  
Souq Area  
Al-Beker  
Turbat Mohammad  
Zuiwaya “Cornerstone”  
Al-Mualimen “Teacher’s”

Al Iskala  
Hai Al-Sana’I “Industrial”  
Cheri  
Hammam “Public Shower District”  
Al-Jabal “Mountain or Hill”  
Al Itfa  
Al Qadaseya  
Khaldeeya  
Al Jamiyah  
Al-Binan “Fingertips”

Outlying Areas:

Muhammadi  
Zuwayyah  
Tal Aswad  
Aqubah  
Abu Tiban  
Kubaysah  
Zughayr  
Hit

Qutbiyah  
Zukhaykhlah  
Nuwayim  
Warshaniyah  
Khasraj  
Sihaliyah  
Wuslah  
Maskhan

All **outlying areas** and the cities/villages in the mentioned **districts** will all fall under the naming convention of **HIT**. In the **ID Number Type** field, **HIT** will be picked from the drop down list (or typed in if not there).

**10. KARMAH**

Regions:

Al Jazirah	Al Jumaylah
Dra Digla	Bani Zaied
Zoba (Hammam)	Lahibi
Albu Khalifah	Halbusi
Shorztan	Zoba (Hammam)

Outlying Areas:

Albu Khamfur	Qaryat Albu Ugool
Qaryat Albu Jassim	Qaryat Al Rashad
Qaryat Albu Sawdah	Jumaylah
Janabin	Qaryat Al Lahib
Ganatar	Qaryat Ash Shahabi
Halabsa	Qaryat Al Libyah
Qaryat Albu Khalifah	Sitcher
Qaryat Albu Awda	

All **outlying areas** and the cities/villages in the mentioned **regions** will all fall under the naming convention of **KARMAH**. In the **ID Number Type** field, **KARMAH** will be picked from the drop down list (or typed in if not there).

**11. CAMP KOREAN VILLAGE/RUTBAH**

Districts:

Al-Karable	Al-Matar
Al-Wadi	Al-Methaq
Al-Hara	Al-Antisar

All cities/villages in the mentioned **districts** will all fall under the naming convention of **RUTBAH**. In the **ID Number Type** field, **RUTBAH** will be picked from the drop down list (or typed in if not there).

**12. LAKE THAR THAR**

All **outlying areas** surrounding Lake Thar Thar will all fall under the naming convention of **THAR THAR**. In the **ID Number Type** field, **THAR THAR** will be picked from the drop down list (or typed in if not there).

**13. NUKHAYB**



## UNCLASSIFIED – FOR OFFICIAL USE ONLY

All **outlying areas** surrounding Nukhayb will all fall under the naming convention of **NUKHAYB**. In the **ID Number Type** field, **NUKHAYB** will be picked from the drop down list (or typed in if not there).

### 14. RAMADI

Districts:

5-Kilo	Al Andols
Ta'meem	Hay Al Dhobot Thanya – 2 <sup>nd</sup> Officer's
Al Warar	Sina'a Industrial
Al Hawz	Al Iskan AKA Police Housing Area
Hay Al Dhobot – 1 <sup>st</sup> Officer's	Al Mala'ab Large Stadium
Thaylat	Albu Jabar
Al Mualemeen	Sufia
Al Shrikah	Zeraa Agricultural
Qatana	

Outlying Areas:

Humayrah	Sajariah
Zangora	Julaybah
Jazirah	Sufia
Jurayshi	

All **outlying areas** and the cities/villages in the mentioned **districts** will all fall under the naming convention of **RAMADI**. In the **ID Number Type** field, **RAMADI** will be picked from the drop down list (or typed in if not there).

### 15. RAWAH

Districts:

Al Qadasiyah	Hilalia
Zarashiyah	Jadiyah (New Rawah)
Al Askari	Qadima (Old Rawah)

All cities/villages in the mentioned **districts** will all fall under the naming convention of **RAWAH**. In the **ID Number Type** field, **RAWAH** will be picked from the drop down list (or typed in if not there).

### 16. REYANAH

All **outlying areas** surrounding Reyanah will all fall under the naming convention of **REYANAH**. In the **ID Number Type** field, **REYANAH** will be picked from the drop down list (or typed in if not there).

### 17. SAQLAWIYAH

Outlying Areas:

Bakhit

Ziggurat

Remallah

North Saqlawiyah

Albu Shijil

Tali'ah

Ahwaiwa

Abu Sudayrah

## UNCLASSIFIED- FOR OFFICIAL USE ONLY

All **outlying areas** surrounding Saqlawiyah will all fall under the naming convention of **SAQLAWIYAH**. In the **ID Number Type** field, **SAQLAWIYAH** will be picked from the drop down list (or typed in if not there).

### 18. TREBIL

All **outlying areas** surrounding Camp Trebil will all fall under the naming convention of **TREBIL**. In the **ID Number Type** field, **TREBIL** will be picked from the drop down list (or typed in if not there).

### 19. ZAIDON

Regions:

West

Northeast

Southeast

All cities/villages in the mentioned **regions** will all fall under the naming convention of **ZAIDON**. In the **ID Number Type** field, **ZAIDON** will be picked from the drop down list (or typed in if not there).

UNCLASSIFIED- FOR OFFICIAL USE ONLY